Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Adobe					
connect					
Deserialization of Untrusted Data	21-Oct-21	7.5	Adobe Connect version 11.2.2 (and earlier) is affected by a Deserialization of Untrusted Data vulnerability to achieve arbitrary method invocation when AMF messages are deserialized on an Adobe Connect server. An attacker can leverage this to execute remote code execution on the server. **CVE ID : CVE-2021-40719**	https://helpx.adobe.com/security/products/connect/apsb21-91.html	A-ADO-CONN-031121/1
Advantech					
webaccess					
Out-of-bounds Write	18-Oct-21	7.5	Advantech WebAccess versions 9.02 and prior are vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute code. **CVE ID : CVE-2021-38389**	N/A	A-ADV-WEBA-031121/2
Out-of-bounds Write	18-Oct-21	7.5	Advantech WebAccess versions 9.02 and prior are vulnerable to a heap-based buffer overflow, which may allow an attacker to remotely execute code. **CVE ID : CVE-2021-33023**	N/A	A-ADV-WEBA-031121/3
webaccess\\/nms					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	27-Oct-21	5	WebAccess/NMS (Versions prior to v3.0.3_Build6299) has an improper authentication vulnerability, which may allow unauthorized users to view resources monitored and controlled by the WebAccess/NMS, as well as IP addresses and names of all the devices managed via WebAccess/NMS. **CVE ID : CVE-2021-32951**	https://us-cert.cisa.gov/ics/advisories/icsa-21-229-02	A-ADV-WEBA-031121/4
Alfresco					
alfresco_content_services					
Exposure of Resource to Wrong Sphere	21-Oct-21	6.5	An issue was discovered in Hyland org.alfresco:alfresco-content-services through 7.0.1.2. Script Action execution allows executing scripts uploaded outside of the Data Dictionary. This could allow a logged-in attacker to execute arbitrary code inside a sandboxed environment. **CVE ID : CVE-2021-41790**	N/A	A-ALF-ALFR-031121/5
Server-Side Request Forgery (SSRF)	21-Oct-21	5	An issue was discovered in Hyland org.alfresco:alfresco-content-services through 6.2.2.18 and org.alfresco:alfresco-transform-services through 1.3. A crafted HTML file, once uploaded, could trigger an unexpected request by the transformation engine. The response to the request is not available to the	N/A	A-ALF-ALFR-031121/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker, i.e., this is blind SSRF. **CVE ID : CVE-2021-41792**		
alfresco_transform_services					
Server-Side Request Forgery (SSRF)	21-Oct-21	5	An issue was discovered in Hyland org.alfresco:alfresco-content-services through 6.2.2.18 and org.alfresco:alfresco-transform-services through 1.3. A crafted HTML file, once uploaded, could trigger an unexpected request by the transformation engine. The response to the request is not available to the attacker, i.e., this is blind SSRF. **CVE ID : CVE-2021-41792**	N/A	A-ALF-ALFR-031121/7
community_share					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	3.5	An issue was discovered in Hyland org.alfresco:share through 7.0.0.2 and org.alfresco:community-share through 7.0. An evasion of the XSS filter for HTML input validation in the Alfresco Share User Interface leads to stored XSS that could be exploited by an attacker (given that he has privileges on the content collaboration features). **CVE ID : CVE-2021-41791**	N/A	A-ALF-COMM-031121/8
share					
Improper Neutralization of Input	21-Oct-21	3.5	An issue was discovered in Hyland org.alfresco:share through 7.0.0.2 and	N/A	A-ALF-SHAR-031121/9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			org.alfresco:community-share through 7.0. An evasion of the XSS filter for HTML input validation in the Alfresco Share User Interface leads to stored XSS that could be exploited by an attacker (given that he has privileges on the content collaboration features). **CVE ID : CVE-2021-41791**		
Alkacon					
opencms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	In "OpenCMS", versions 10.5.0 to 11.0.2 are affected by a stored XSS vulnerability that allows low privileged application users to store malicious scripts in the Sitemap functionality. These scripts are executed in a victim's browser when they open the page containing the vulnerable field. **CVE ID : CVE-2021-25968**	https://github.com/alkacon/mercury-template/commit/800945f5d02346c633c7aef9f5d596d7dedc8fb5	A-ALK-OPEN-031121/10
Amazon					
tough					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-21	8.5	Tough provides a set of Rust libraries and tools for using and generating the update framework (TUF) repositories. The tough library, prior to 0.12.0, does not properly sanitize target names when caching a repository, or when saving specific targets to an output directory. When targets are	https://github.com/awslabs/tough/security/advisories/GHSA-x3r5-q6mj-m485, https://github.com/awslabs/tough/commit/1809b	A-AMA-TOUG-031121/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cached or saved, files could be overwritten with arbitrary content anywhere on the system. A fix is available in version 0.12.0. No workarounds to this issue are known. **CVE ID : CVE-2021-41149**	9bd1106d78a51fbea3071aa97a3530bac9a	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-21	3.5	Tough provides a set of Rust libraries and tools for using and generating the update framework (TUF) repositories. The tough library, prior to 0.12.0, does not properly sanitize delegated role names when caching a repository, or when loading a repository from the filesystem. When the repository is cached or loaded, files ending with the .json extension could be overwritten with role metadata anywhere on the system. A fix is available in version 0.12.0. No workarounds to this issue are known. **CVE ID : CVE-2021-41150**	https://github.com/awslabs/tough/security/advisories/GHSA-r56q-vv3c-6g9c, https://github.com/awslabs/tough/commit/1809b9bd1106d78a51fbea3071aa97a3530bac9a	A-AMA-TOUG-031121/12
anaconda					
dask					
Exposure of Resource to Wrong Sphere	26-Oct-21	6.8	An issue was discovered in Dask (aka python-dask) through 2021.09.1. Single machine Dask clusters started with dask.distributed.LocalCluster or dask.distributed.Client (which defaults to using	https://docs.dask.org/en/latest/changelog.html	A-ANA-DASK-031121/13

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			LocalCluster) would mistakenly configure their respective Dask workers to listen on external interfaces (typically with a randomly selected high port) rather than only on localhost. A Dask cluster created using this method (when running on a machine that has an applicable port exposed) could be used by a sophisticated attacker to achieve remote code execution. **CVE ID : CVE-2021-42343**		
antsword_redis_project					
antsword_redis					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-21	3.5	AS_Redis is an AntSword plugin for Redis. The Redis Manage plugin for AntSword prior to version 0.5 is vulnerable to Self-XSS due to due to insufficient input validation and sanitization via redis server configuration. Self-XSS in the plugin configuration leads to code execution. This issue is patched in version 0.5. **CVE ID : CVE-2021-41172**	https://github.com/Medicean/AS_Redis/security/advisories/GHSA-j8j6-f829-w425	A-ANT-ANTS-031121/14
Apache					
storm					
Improper Neutralization of Special Elements in Output Used	25-Oct-21	7.5	A Command Injection vulnerability exists in the getTopologyHistory service of the Apache Storm 2.x prior to 2.2.1 and Apache	https://lists.apache.org/thread.html/r5fe881f6ca883908b7a0f	A-APA-STOR-031121/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			Storm 1.x prior to 1.2.4. A specially crafted thrift request to the Nimbus server allows Remote Code Execution (RCE) prior to authentication. **CVE ID : CVE-2021-38294**	005d35115af49f43beea7a8b0915e377859%40%3Cuser.storm.apache.org%3E	
Deserialization of Untrusted Data	25-Oct-21	7.5	An Unsafe Deserialization vulnerability exists in the worker services of the Apache Storm supervisor server allowing pre-auth Remote Code Execution (RCE). Apache Storm 2.2.x users should upgrade to version 2.2.1 or 2.3.0. Apache Storm 2.1.x users should upgrade to version 2.1.1. Apache Storm 1.x users should upgrade to version 1.2.4 **CVE ID : CVE-2021-40865**	https://lists.apache.org/thread.html/r8d45e74299897b6734dd0f788c46a631009ce2eeb731523386f7a253%40%3Cuser.storm.apache.org%3E	A-APA-STOR-031121/16
superset					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Oct-21	6	Apache Superset up to and including 1.3.0 when configured with ENABLE_TEMPLATE_PROCESSING on (disabled by default) allowed SQL injection when a malicious authenticated user sends an http request with a custom URL. **CVE ID : CVE-2021-41971**	https://lists.apache.org/thread.html/rf7292731268c6c6e2196ae1583e32ac7189385364268f8d9215e8e6d%40%3Cdev.superset.apache.org%3E	A-APA-SUPE-031121/17
Improper Neutralization of Input During Web	18-Oct-21	3.5	Apache Superset up to and including 1.1 does not sanitize titles correctly on the Explore page. This allows	https://lists.apache.org/thread.html/r2c09254e98	A-APA-SUPE-031121/18

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			an attacker with Explore access to save a chart with a malicious title, injecting html (including scripts) into the page. **CVE ID : CVE-2021-32609**	b4f8b3deb422762bd0e2aa6d743b72d96c2f90cbaae31a%40%3Cdev.superset.apache.org%3E	
Apple					
itunes					
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in Security Update 2021-005 Catalina, iTunes 12.12 for Windows, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30835**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	A-APP-ITUN-031121/19
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in watchOS 8, macOS Big Sur 11.6, Security Update 2021-005 Catalina,	https://support.apple.com/en-us/HT212819,	A-APP-ITUN-031121/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30847**	https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
Out-of-bounds Write	19-Oct-21	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, watchOS 8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-30849**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212807, https://supp	A-APP-ITUN-031121/21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212816, https://support.apple.com/en-us/HT212814	
safari					
Out-of-bounds Write	19-Oct-21	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-30846**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212816, https://support.apple.com/en-us/HT212814	A-APP-SAFA-031121/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-21	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, Safari 15, iOS 15 and iPadOS 15. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2021-30848**	https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212816, https://support.apple.com/en-us/HT212814	A-APP-SAFA-031121/23
Out-of-bounds Write	19-Oct-21	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, watchOS 8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-30849**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212816, https://supp	A-APP-SAFA-031121/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT212814	
Atlassian					
jira					
Cross-Site Request Forgery (CSRF)	21-Oct-21	6.8	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to modify various resources via a Cross-Site Request Forgery (CSRF) vulnerability, following an Information Disclosure vulnerability in the referrer headers which discloses a user's CSRF token. The affected versions are before version 8.5.10, and from version 8.6.0 before 8.13.2. **CVE ID : CVE-2021-39126**	https://jira.atlassian.com/browse/JRASERVER-71806	A-ATL-JIRA-031121/25
Exposure of Resource to Wrong Sphere	21-Oct-21	5	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to the query component JQL endpoint via a Broken Access Control vulnerability (BAC) vulnerability. The affected versions are before version 8.5.10, and from version 8.6.0 before 8.13.1. **CVE ID : CVE-2021-39127**	https://jira.atlassian.com/browse/JRASERVER-72003	A-ATL-JIRA-031121/26
Improper Neutralization of Input During Web Page	26-Oct-21	4.3	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to inject arbitrary	https://jira.atlassian.com/browse/JRASERVER-	A-ATL-JIRA-031121/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the /secure/admin/ImporterFinishedPage.jspa error message. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.1. **CVE ID : CVE-2021-41304**	72939	
Exposure of Sensitive Information to an Unauthorized Actor	26-Oct-21	5	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to view the names of private projects and filters via an Insecure Direct Object References (IDOR) vulnerability in the Average Number of Times in Status Gadget. The affected versions are before version 8.13.12.. **CVE ID : CVE-2021-41305**	https://jira.atlassian.com/browse/JRASERVER-72813	A-ATL-JIRA-031121/28
Exposure of Sensitive Information to an Unauthorized Actor	26-Oct-21	5	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to view private project and filter names via an Insecure Direct Object References (IDOR) vulnerability in the Average Time in Status Gadget. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.0. **CVE ID : CVE-2021-41306**	https://jira.atlassian.com/browse/JRASERVER-72915	A-ATL-JIRA-031121/29
Authorization	26-Oct-21	5	Affected versions of	https://jira.a	A-ATL-JIRA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bypass Through User-Controlled Key			Atlassian Jira Server and Data Center allow unauthenticated remote attackers to view the names of private projects and private filters via an Insecure Direct Object References (IDOR) vulnerability in the Workload Pie Chart Gadget. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.0. **CVE ID : CVE-2021-41307**	tlassian.com /browse/JRASERVER-72916	031121/30
Improper Authenticatio n	26-Oct-21	4	Affected versions of Atlassian Jira Server and Data Center allow authenticated yet non-administrator remote attackers to edit the File Replication settings via a Broken Access Control vulnerability in the `ReplicationSettings!default.jspa` endpoint. The affected versions are before version 8.6.0, from version 8.7.0 before 8.13.12, and from version 8.14.0 before 8.20.1. **CVE ID : CVE-2021-41308**	https://jira.atlassian.com /browse/JRASERVER-72940	A-ATL-JIRA-031121/31
jira_software_data_center					
Cross-Site Request Forgery (CSRF)	21-Oct-21	6.8	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to modify various resources via a Cross-Site Request Forgery (CSRF) vulnerability, following an	https://jira.atlassian.com /browse/JRASERVER-71806	A-ATL-JIRA-031121/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure vulnerability in the referrer headers which discloses a user's CSRF token. The affected versions are before version 8.5.10, and from version 8.6.0 before 8.13.2. **CVE ID : CVE-2021-39126**		
Exposure of Resource to Wrong Sphere	21-Oct-21	5	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to the query component JQL endpoint via a Broken Access Control vulnerability (BAC) vulnerability. The affected versions are before version 8.5.10, and from version 8.6.0 before 8.13.1. **CVE ID : CVE-2021-39127**	https://jira.atlassian.com/browse/JRASERVER-72003	A-ATL-JIRA-031121/33
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-21	4.3	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the /secure/admin/ImporterFinishedPage.jspa error message. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.1. **CVE ID : CVE-2021-41304**	https://jira.atlassian.com/browse/JRASERVER-72939	A-ATL-JIRA-031121/34
Exposure of Sensitive Information	26-Oct-21	5	Affected versions of Atlassian Jira Server and Data Center allow	https://jira.atlassian.com/browse/JRA	A-ATL-JIRA-031121/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to an Unauthorized Actor			anonymous remote attackers to view the names of private projects and filters via an Insecure Direct Object References (IDOR) vulnerability in the Average Number of Times in Status Gadget. The affected versions are before version 8.13.12.. **CVE ID : CVE-2021-41305**	SERVER-72813	
Exposure of Sensitive Information to an Unauthorized Actor	26-Oct-21	5	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to view private project and filter names via an Insecure Direct Object References (IDOR) vulnerability in the Average Time in Status Gadget. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.0. **CVE ID : CVE-2021-41306**	https://jira.atlassian.com/browse/JRASERVER-72915	A-ATL-JIRA-031121/36
Authorization Bypass Through User-Controlled Key	26-Oct-21	5	Affected versions of Atlassian Jira Server and Data Center allow unauthenticated remote attackers to view the names of private projects and private filters via an Insecure Direct Object References (IDOR) vulnerability in the Workload Pie Chart Gadget. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.0.	https://jira.atlassian.com/browse/JRASERVER-72916	A-ATL-JIRA-031121/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-41307		
Improper Authentication	26-Oct-21	4	Affected versions of Atlassian Jira Server and Data Center allow authenticated yet non-administrator remote attackers to edit the File Replication settings via a Broken Access Control vulnerability in the `ReplicationSettings!default.jspa` endpoint. The affected versions are before version 8.6.0, from version 8.7.0 before 8.13.12, and from version 8.14.0 before 8.20.1. **CVE ID : CVE-2021-41308**	https://jira.atlassian.com/browse/JRASERVER-72940	A-ATL-JIRA-031121/38
automatedlogic					
webctrl					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-21	4.3	The login portal for the Automated Logic WebCTRL/WebCTRL OEM web application contains a vulnerability that allows for reflected XSS attacks due to the operatorlocale GET parameter not being sanitized. This issue impacts versions 6.5 and below. This issue works by passing in a basic XSS payload to a vulnerable GET parameter that is reflected in the output without sanitization. **CVE ID : CVE-2021-31682**	https://www.automatedlogic.com/en/products-services/webctrl-building-automation-system/	A-AUT-WEBC-031121/39
auvesy					
versiondog					
Write-what-	22-Oct-21	7.5	Some API functions permit	https://us-	A-AUV-VERS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
where Condition			by-design writing or copying data into a given buffer. Since the client controls these parameters, an attacker could rewrite the memory in any location of the affected product. **CVE ID : CVE-2021-38449**	cert.cisa.gov/ics/advisories/icsa-21-292-01	031121/40
Out-of-bounds Read	22-Oct-21	3.5	The affected product's proprietary protocol CSC allows for calling numerous function codes. In order to call those function codes, the user must supply parameters. There is no sanitation on the value of the offset, which allows the client to specify any offset and read out-of-bounds data. **CVE ID : CVE-2021-38451**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/41
External Control of System or Configuration Setting	22-Oct-21	6.4	Some API functions allow interaction with the registry, which includes reading values as well as data modification. **CVE ID : CVE-2021-38453**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/42
Improper Input Validation	22-Oct-21	4	The affected product's OS Service does not verify any given parameter. A user can supply any type of parameter that will be passed to inner calls without checking the type of the parameter or the value. **CVE ID : CVE-2021-38455**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/43
Improper Access Control	22-Oct-21	7.5	The server permits communication without any authentication procedure, allowing the attacker to	https://us-cert.cisa.gov/ics/advisories/icsa-21-	A-AUV-VERS-031121/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			initiate a session with the server without providing any form of authentication. **CVE ID : CVE-2021-38457**	292-01	
Authentication Bypass by Capture-replay	22-Oct-21	7.5	The data of a network capture of the initial handshake phase can be used to authenticate at a SYSDBA level. If a specific .exe is not restarted often, it is possible to access the needed handshake packets between admin/client connections. Using the SYSDBA permission, an attacker can change user passwords or delete the database. **CVE ID : CVE-2021-38459**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/45
Use of Hard-coded Cryptographic Key	22-Oct-21	6.4	The affected product uses a hard-coded blowfish key for encryption/decryption processes. The key can be easily extracted from binaries. **CVE ID : CVE-2021-38461**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/46
Uncontrolled Resource Consumption	22-Oct-21	5.5	The affected product does not properly control the allocation of resources. A user may be able to allocate unlimited memory buffers using API functions. **CVE ID : CVE-2021-38463**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/47
Uncontrolled Resource Consumption	22-Oct-21	4	The webinstaller is a Golang web server executable that enables the generation of an Auvesy image agent. Resource consumption can be achieved by generating	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			large amounts of installations, which are then saved without limitation in the temp folder of the webinstaller executable. **CVE ID : CVE-2021-38465**		
Use After Free	22-Oct-21	5.5	A specific function code receives a raw pointer supplied by the user and deallocates this pointer. The user can then control what memory regions will be freed and cause use-after-free condition. **CVE ID : CVE-2021-38467**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/49
Uncontrolled Search Path Element	22-Oct-21	4.3	Many of the services used by the affected product do not specify full paths for the DLLs they are loading. An attacker can exploit the uncontrolled search path by implanting their own DLL near the affected product's binaries, thus hijacking the loaded DLL. **CVE ID : CVE-2021-38469**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/50
Unrestricted Upload of File with Dangerous Type	22-Oct-21	6.4	There are multiple API function codes that permit data writing to any file, which may allow an attacker to modify existing files or create new files. **CVE ID : CVE-2021-38471**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/51
Improper Restriction of Operations within the Bounds of a Memory	22-Oct-21	6.5	The affected product's code base doesn't properly control arguments for specific functions, which could lead to a stack	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			overflow. **CVE ID : CVE-2021-38473**		
Incorrect Permission Assignment for Critical Resource	22-Oct-21	9	The database connection to the server is performed by calling a specific API, which could allow an unprivileged user to gain SYSDBA permissions. **CVE ID : CVE-2021-38475**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/53
External Control of File Name or Path	22-Oct-21	6.4	There are multiple API function codes that permit reading and writing data to or from files and directories, which could lead to the manipulation and/or the deletion of files. **CVE ID : CVE-2021-38477**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/54
Out-of-bounds Write	22-Oct-21	5	Many API function codes receive raw pointers remotely from the user and trust these pointers as valid in-bound memory regions. An attacker can manipulate API functions by writing arbitrary data into the resolved address of a raw pointer. **CVE ID : CVE-2021-38479**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/55
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Oct-21	7.5	The scheduler service running on a specific TCP port enables the user to start and stop jobs. There is no sanitation of the supplied JOB ID provided to the function. An attacker may send a malicious payload that can enable the user to execute another SQL expression by sending a	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01	A-AUV-VERS-031121/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific string. **CVE ID : CVE-2021-38481**		
Bestpractical					
request_tracker					
Observable Discrepancy	18-Oct-21	5	Best Practical Request Tracker (RT) 4.2 before 4.2.17, 4.4 before 4.4.5, and 5.0 before 5.0.2 allows sensitive information disclosure via a timing attack against lib/RT/REST2/Middleware/Auth.pm. **CVE ID : CVE-2021-38562**	https://docs.bestpractical.com/release-notes/rt/index.html, https://github.com/bestpractical/rt/commit/70749bb66cb13dd70bd53340c371038a5f3ca57c	A-BES-REQU-031121/57
binaryops					
x-assign					
Improperly Controlled Modification of Dynamically-Determined Object Attributes	20-Oct-21	7.5	This affects all versions of package x-assign. The global proto object can be polluted using the __proto__ object. **CVE ID : CVE-2021-23452**	N/A	A-BIN-X-AS-031121/58
bludit					
bludit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	4.3	Cross Site Scripting (XSS) vulnerability exists in bludit 3-13-1 via the username in admin/login. **CVE ID : CVE-2021-35323**	N/A	A-BLU-BLUD-031121/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bplugins					
easy_twitter_feed					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	The Easy Twitter Feed WordPress plugin before 1.2 does not sanitise or validate the parameters from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them which will be triggered in the page/s with the embed malicious shortcode **CVE ID : CVE-2021-24413**	N/A	A-BPL-EASY-031121/60
html5_audio_player					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	The Html5 Audio Player â€“ Audio Player for WordPress plugin before 2.1.3 does not sanitise or validate the parameters from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them which will be triggered in the page/s with the embed malicious shortcode **CVE ID : CVE-2021-24412**	N/A	A-BPL-HTML-031121/61
polo_video_gallery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	The Polo Video Gallery â€“ Best wordpress video gallery plugin WordPress plugin through 1.2 does not sanitise or validate the parameters from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them	N/A	A-BPL-POLO-031121/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which will be triggered in the page/s with the embed malicious shortcode **CVE ID : CVE-2021-24415**		
streamcast_radio_player					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	The StreamCast â€“ Radio Player for WordPress plugin before 2.1.1 does not sanitise or validate the parameters from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them which will be triggered in the page/s with the embed malicious shortcode **CVE ID : CVE-2021-24416**	N/A	A-BPL-STRE-031121/63
bqe					
billquick_web_suite					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Oct-21	6.8	BQE BillQuick Web Suite 2018 through 2021 before 22.0.9.1 allows SQL injection for unauthenticated remote code execution, as exploited in the wild in October 2021 for ransomware installation. SQL injection can, for example, use the txtID (aka username) parameter. Successful exploitation can include the ability to execute arbitrary code as MSSQLSERVER$ via xp_cmdshell. **CVE ID : CVE-2021-42258**	N/A	A-BQE-BILL-031121/64
catchplugins					
catch_scroll_progress_bar					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	18-Oct-21	3.5	Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_switch AJAX action, which could allow any authenticated users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9, To Top WordPress plugin before 2.3, Header Enhancement WordPress plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations.	N/A	A-CAT-CATC-031121/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24752		
catch_sticky_menu					
Cross-Site Request Forgery (CSRF)	18-Oct-21	3.5	Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_switch AJAX action, which could allow any authenticated users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9, To Top WordPress plugin before 2.3, Header Enhancement WordPress plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb	N/A	A-CAT-CATC-031121/66

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations. **CVE ID : CVE-2021-24752**		
catch_themes_demo_import					
Unrestricted Upload of File with Dangerous Type	21-Oct-21	6.5	The Catch Themes Demo Import WordPress plugin is vulnerable to arbitrary file uploads via the import functionality found in the ~/inc/CatchThemesDemoImport.php file, in versions up to and including 1.7, due to insufficient file type validation. This makes it possible for an attacker with administrative privileges to upload malicious files that can be used to achieve remote code execution. **CVE ID : CVE-2021-39352**	https://plugins.trac.wordpress.org/changeset/2617555/catch-themes-demo-import/trunk/inc/CatchThemesDemoImport.php	A-CAT-CATC-031121/67
Cross-Site Request Forgery (CSRF)	18-Oct-21	3.5	Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_switch AJAX action, which could allow any authenticated users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9, To Top WordPress plugin before 2.3, Header Enhancement WordPress plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin	N/A	A-CAT-CATC-031121/68

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations. **CVE ID : CVE-2021-24752**		
catch_under_construction					
Cross-Site Request Forgery (CSRF)	18-Oct-21	3.5	Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_switch AJAX action, which could allow any authenticated users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9, To Top WordPress plugin before 2.3, Header Enhancement WordPress plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential	N/A	A-CAT-CATC-031121/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations. **CVE ID : CVE-2021-24752**		
catch_web_tools					
Cross-Site Request Forgery (CSRF)	18-Oct-21	3.5	Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_switch AJAX action, which could allow any authenticated users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9, To Top WordPress plugin before 2.3, Header Enhancement WordPress	N/A	A-CAT-CATC-031121/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations. **CVE ID : CVE-2021-24752**		
essential_content_types					
Cross-Site Request Forgery (CSRF)	18-Oct-21	3.5	Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_switch AJAX action, which could allow any authenticated users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9,	N/A	A-CAT-ESSE-031121/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			To Top WordPress plugin before 2.3, Header Enhancement WordPress plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations. **CVE ID : CVE-2021-24752**		
essential_widgets					
Cross-Site Request Forgery (CSRF)	18-Oct-21	3.5	Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_switch AJAX action, which could allow any authenticated	N/A	A-CAT-ESSE-031121/72

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9, To Top WordPress plugin before 2.3, Header Enhancement WordPress plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations. **CVE ID : CVE-2021-24752**		
generate_child_theme					
Cross-Site Request Forgery	18-Oct-21	3.5	Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF	N/A	A-CAT-GENE-031121/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			checks in the ctp_switch AJAX action, which could allow any authenticated users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9, To Top WordPress plugin before 2.3, Header Enhancement WordPress plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations. **CVE ID : CVE-2021-24752**		
header_enhancement					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	18-Oct-21	3.5	Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_switch AJAX action, which could allow any authenticated users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9, To Top WordPress plugin before 2.3, Header Enhancement WordPress plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations.	N/A	A-CAT-HEAD-031121/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24752		
to_top					
Cross-Site Request Forgery (CSRF)	18-Oct-21	3.5	Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_switch AJAX action, which could allow any authenticated users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9, To Top WordPress plugin before 2.3, Header Enhancement WordPress plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb	N/A	A-CAT-TO_T-031121/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations. **CVE ID : CVE-2021-24752**		
Checkpoint					
harmony_browse					
Uncontrolled Search Path Element	22-Oct-21	7.2	The Harmony Browse and the SandBlast Agent for Browsers installers must have admin privileges to execute some steps during the installation. Because the MS Installer allows regular users to repair their installation, an attacker running an installer before 90.08.7405 can start the installation repair and place a specially crafted binary in the repair folder, which runs with the admin privileges. **CVE ID : CVE-2021-30359**	https://supportcontent.checkpoint.com/solutions?id=sk175968	A-CHE-HARM-031121/76
mobile_access_portal_agent					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-21	6	Mobile Access Portal Native Applications who's path is defined by the administrator with environment variables may run applications from other locations by the Mobile Access Portal Agent. **CVE ID : CVE-2021-30358**	https://supportcontent.checkpoint.com/solutions?id=sk175806, https://supportcontent.checkpoint.com/solutions?id=sk142952	A-CHE-MOBI-031121/77
sandblast_agent_for_browsers					
Uncontrolled Search Path Element	22-Oct-21	7.2	The Harmony Browse and the SandBlast Agent for Browsers installers must have admin privileges to	https://supportcontent.checkpoint.com/solutions?id	A-CHE-SAND-031121/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute some steps during the installation. Because the MS Installer allows regular users to repair their installation, an attacker running an installer before 90.08.7405 can start the installation repair and place a specially crafted binary in the repair folder, which runs with the admin privileges. **CVE ID : CVE-2021-30359**	=sk175968	
cimatti					
contact_forms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-21	3.5	The WordPress Contact Forms by Cimatti WordPress plugin before 1.4.12 does not sanitise and escape the Form Title before outputting it in some admin pages. which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed. **CVE ID : CVE-2021-24744**	N/A	A-CIM-CONT-031121/79
Cisco					
adaptive_security_appliance					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	A-CIS-ADAP-031121/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**		
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	A-CIS-ADAP-031121/81

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	A-CIS-ADAP-031121/82
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	A-CIS-ADAP-031121/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	A-CIS-ADAP-031121/84
Improper Enforcement of Message	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA)	https://tools.cisco.com/security/center	A-CIS-ADAP-031121/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integrity During Transmission in a Communication Channel			Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**	/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	A-CIS-ADAP-031121/86

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	A-CIS-ADAP-031121/87
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-ADAP-031121/88

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	sa-asafdt-webvpn-dos-KSqJAKPA	
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	A-CIS-ADAP-031121/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**		
firepower_management_center					
N/A	27-Oct-21	5	Multiple vulnerabilities in the payload inspection for Ethernet Industrial Protocol (ENIP) traffic for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured rules for ENIP traffic. These vulnerabilities are due to incomplete processing during deep packet inspection for ENIP packets. An attacker could exploit these vulnerabilities by sending a crafted ENIP packet to the targeted interface. A successful exploit could allow the attacker to bypass configured access control and intrusion policies that should be activated for the ENIP packet. **CVE ID : CVE-2021-34754**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-enip-bypass-eFsxd8KP	A-CIS-FIRE-031121/90
Missing Release of Memory after Effective Lifetime	27-Oct-21	7.8	Multiple Cisco products are affected by a vulnerability in the way the Snort detection engine processes ICMP traffic that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-s2R7W9UU	A-CIS-FIRE-031121/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper memory resource management while the Snort detection engine is processing ICMP packets. An attacker could exploit this vulnerability by sending a series of ICMP packets through an affected device. A successful exploit could allow the attacker to exhaust resources on the affected device, causing the device to reload. **CVE ID : CVE-2021-40114**		
N/A	27-Oct-21	7.1	Multiple Cisco products are affected by a vulnerability in Snort rules that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.The vulnerability is due to improper handling of the Block with Reset or Interactive Block with Reset actions if a rule is configured without proper constraints. An attacker could exploit this vulnerability by sending a crafted IP packet to the affected device. A successful exploit could allow the attacker to cause through traffic to be dropped. Note: Only products with Snort3 configured and either a rule with Block with Reset or Interactive Block with Reset actions configured are	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-RywH7ezM	A-CIS-FIRE-031121/92

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerable. Products configured with Snort2 are not vulnerable. **CVE ID : CVE-2021-40116**		
firepower_management_center_virtual_appliance					
Improper Input Validation	27-Oct-21	7.2	Multiple vulnerabilities in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34755**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-cmdinject-FmzsLN8	A-CIS-FIRE-031121/93
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Oct-21	7.2	Multiple vulnerabilities in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34756**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-cmdinject-FmzsLN8	A-CIS-FIRE-031121/94
Improper Input Validation	27-Oct-21	6.6	A vulnerability in Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to overwrite or append arbitrary data to system files using root-level privileges. The attacker must	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-file-write-	A-CIS-FIRE-031121/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have administrative credentials on the device. This vulnerability is due to incomplete validation of user input for a specific CLI command. An attacker could exploit this vulnerability by authenticating to the device with administrative privileges and issuing a CLI command with crafted user parameters. A successful exploit could allow the attacker to overwrite or append arbitrary data to system files using root-level privileges. **CVE ID : CVE-2021-34761**	SHVcmQVc	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Oct-21	5.5	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to perform a directory traversal attack on an affected device. The attacker would require valid device credentials. The vulnerability is due to insufficient input validation of the HTTPS URL by the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTPS request that contains directory traversal character sequences to an affected device. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-dir-traversal-95UyW5tk	A-CIS-FIRE-031121/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to read or write arbitrary files on the device. **CVE ID : CVE-2021-34762**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an attacker to execute a cross-site scripting (XSS) attack or an open redirect attack. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34763**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-openredir-TVPMWJyg	A-CIS-FIRE-031121/97
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	5.8	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an attacker to execute a cross-site scripting (XSS) attack or an open redirect attack. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34764**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-openredir-TVPMWJyg	A-CIS-FIRE-031121/98
Improper Handling of Exceptional Conditions	27-Oct-21	7.1	A vulnerability in the processing of SSH connections for multi-instance deployments of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-rUDseW3r	A-CIS-FIRE-031121/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on the affected device. This vulnerability is due to a lack of proper error handling when an SSH session fails to be established. An attacker could exploit this vulnerability by sending a high rate of crafted SSH connections to the instance. A successful exploit could allow the attacker to cause resource exhaustion, which causes a DoS condition on the affected device. The device must be manually reloaded to recover. **CVE ID : CVE-2021-34781**		
firepower_threat_defense					
N/A	27-Oct-21	5	Multiple vulnerabilities in the payload inspection for Ethernet Industrial Protocol (ENIP) traffic for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured rules for ENIP traffic. These vulnerabilities are due to incomplete processing during deep packet inspection for ENIP packets. An attacker could exploit these vulnerabilities by sending a crafted ENIP packet to the targeted interface. A successful exploit could allow the attacker to bypass configured access control	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-enip-bypass-eFsxd8KP	A-CIS-FIRE-031121/100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and intrusion policies that should be activated for the ENIP packet. **CVE ID : CVE-2021-34754**		
Improper Input Validation	27-Oct-21	7.2	Multiple vulnerabilities in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34755**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-cmdinject-FmzsLN8	A-CIS-FIRE-031121/101
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Oct-21	7.2	Multiple vulnerabilities in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34756**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-cmdinject-FmzsLN8	A-CIS-FIRE-031121/102
Improper Input Validation	27-Oct-21	6.6	A vulnerability in Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to overwrite or append arbitrary data to system files using root-level privileges. The attacker must have administrative	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-file-write-SHVcmQVc	A-CIS-FIRE-031121/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials on the device. This vulnerability is due to incomplete validation of user input for a specific CLI command. An attacker could exploit this vulnerability by authenticating to the device with administrative privileges and issuing a CLI command with crafted user parameters. A successful exploit could allow the attacker to overwrite or append arbitrary data to system files using root-level privileges. **CVE ID : CVE-2021-34761**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Oct-21	5.5	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to perform a directory traversal attack on an affected device. The attacker would require valid device credentials. The vulnerability is due to insufficient input validation of the HTTPS URL by the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTPS request that contains directory traversal character sequences to an affected device. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-dir-traversal-95UyW5tk	A-CIS-FIRE-031121/104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read or write arbitrary files on the device. **CVE ID : CVE-2021-34762**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an attacker to execute a cross-site scripting (XSS) attack or an open redirect attack. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34763**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-openredir-TVPMWJyg	A-CIS-FIRE-031121/105
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	5.8	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an attacker to execute a cross-site scripting (XSS) attack or an open redirect attack. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34764**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-openredir-TVPMWJyg	A-CIS-FIRE-031121/106
Improper Handling of Exceptional Conditions	27-Oct-21	7.1	A vulnerability in the processing of SSH connections for multi-instance deployments of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-rUDseW3r	A-CIS-FIRE-031121/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device. This vulnerability is due to a lack of proper error handling when an SSH session fails to be established. An attacker could exploit this vulnerability by sending a high rate of crafted SSH connections to the instance. A successful exploit could allow the attacker to cause resource exhaustion, which causes a DoS condition on the affected device. The device must be manually reloaded to recover. **CVE ID : CVE-2021-34781**		
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	A-CIS-FIRE-031121/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**		
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	A-CIS-FIRE-031121/109
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-FIRE-031121/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	sa-natalg-bypass-cpKGqkng	
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	A-CIS-FIRE-031121/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	A-CIS-FIRE-031121/112
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	A-CIS-FIRE-031121/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**		
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	A-CIS-FIRE-031121/114
Missing	27-Oct-21	7.8	Multiple Cisco products are	https://tools.	A-CIS-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Release of Memory after Effective Lifetime			affected by a vulnerability in the way the Snort detection engine processes ICMP traffic that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper memory resource management while the Snort detection engine is processing ICMP packets. An attacker could exploit this vulnerability by sending a series of ICMP packets through an affected device. A successful exploit could allow the attacker to exhaust resources on the affected device, causing the device to reload. **CVE ID : CVE-2021-40114**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-s2R7W9UU	031121/115
N/A	27-Oct-21	7.1	Multiple Cisco products are affected by a vulnerability in Snort rules that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.The vulnerability is due to improper handling of the Block with Reset or Interactive Block with Reset actions if a rule is configured without proper constraints. An attacker could exploit this vulnerability by sending a crafted IP packet to the affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-RywH7ezM	A-CIS-FIRE-031121/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause through traffic to be dropped. Note: Only products with Snort3 configured and either a rule with Block with Reset or Interactive Block with Reset actions configured are vulnerable. Products configured with Snort2 are not vulnerable. **CVE ID : CVE-2021-40116**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	A-CIS-FIRE-031121/117
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-FIRE-031121/118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	sa-asafdt-webvpn-dos-KSqJAKPA	
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	A-CIS-FIRE-031121/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**		
identity_services_engine					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34738**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss1-rgxYry2V	A-CIS-IDEN-031121/120
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-40121**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss1-rgxYry2V	A-CIS-IDEN-031121/121
Incorrect Default Permissions	21-Oct-21	4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker with administrative	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-IDEN-031121/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read-only privileges to download files that should be restricted. This vulnerability is due to incorrect permissions settings on an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request to the device. A successful exploit could allow the attacker to download files that should be restricted. **CVE ID : CVE-2021-40123**	sa-ise-file-download-B3BR5KQA	
ios_xe					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	A-CIS-IOS_-031121/123
meeting_server					
Improper Resource	21-Oct-21	5	A vulnerability in an API of the Call Bridge feature of	https://tools.cisco.com/se	A-CIS-MEET-031121/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			Cisco Meeting Server could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper handling of large series of message requests. An attacker could exploit this vulnerability by sending a series of messages to the vulnerable API. A successful exploit could allow the attacker to cause the affected device to reload, dropping all ongoing calls and resulting in a DoS condition. **CVE ID : CVE-2021-40122**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-cms-LAHe8z5v	
sourcefire_defense_center					
Improper Input Validation	27-Oct-21	7.2	Multiple vulnerabilities in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34755**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-cmdinject-FmzsLN8	A-CIS-SOUR-031121/125
Improper Neutralization of Special Elements used in a Command ('Command	27-Oct-21	7.2	Multiple vulnerabilities in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with root	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-	A-CIS-SOUR-031121/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			privileges. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34756**	cmdinject-FmzsLN8	
Improper Input Validation	27-Oct-21	6.6	A vulnerability in Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to overwrite or append arbitrary data to system files using root-level privileges. The attacker must have administrative credentials on the device. This vulnerability is due to incomplete validation of user input for a specific CLI command. An attacker could exploit this vulnerability by authenticating to the device with administrative privileges and issuing a CLI command with crafted user parameters. A successful exploit could allow the attacker to overwrite or append arbitrary data to system files using root-level privileges. **CVE ID : CVE-2021-34761**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-file-write-SHVcmQVc	A-CIS-SOUR-031121/127
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Oct-21	5.5	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to perform a directory traversal attack on	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-dir-traversal-	A-CIS-SOUR-031121/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. The attacker would require valid device credentials. The vulnerability is due to insufficient input validation of the HTTPS URL by the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTPS request that contains directory traversal character sequences to an affected device. A successful exploit could allow the attacker to read or write arbitrary files on the device. **CVE ID : CVE-2021-34762**	95UyW5tk	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an attacker to execute a cross-site scripting (XSS) attack or an open redirect attack. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34763**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-openredir-TVPMWJyg	A-CIS-SOUR-031121/129
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	5.8	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an attacker to execute a cross-site scripting (XSS) attack or an open redirect attack. For more information about	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-openredir-TVPMWJyg	A-CIS-SOUR-031121/130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-34764**		
Improper Handling of Exceptional Conditions	27-Oct-21	7.1	A vulnerability in the processing of SSH connections for multi-instance deployments of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the affected device. This vulnerability is due to a lack of proper error handling when an SSH session fails to be established. An attacker could exploit this vulnerability by sending a high rate of crafted SSH connections to the instance. A successful exploit could allow the attacker to cause resource exhaustion, which causes a DoS condition on the affected device. The device must be manually reloaded to recover. **CVE ID : CVE-2021-34781**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-rUDseW3r	A-CIS-SOUR-031121/131
telepresence_management_suite					
Improper Neutralization of Input During Web Page Generation ('Cross-site	21-Oct-21	3.5	A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) Software could allow an authenticated, remote attacker to conduct a cross-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tms-xss-	A-CIS-TELE-031121/132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data in a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2021-34760**	CwjZJSQc	
tetration					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	3.5	A vulnerability in the web-based management interface of Cisco Tetration could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack on an affected system. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sec-work-xss-t6SYtu8Q	A-CIS-TETR-031121/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			To exploit this vulnerability, the attacker would need valid administrative credentials. **CVE ID : CVE-2021-34789**		
unified_computing_system					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	A-CIS-UNIF-031121/134
unified_threat_defense					
Missing Release of Memory after Effective Lifetime	27-Oct-21	7.8	Multiple Cisco products are affected by a vulnerability in the way the Snort detection engine processes ICMP traffic that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-s2R7W9UU	A-CIS-UNIF-031121/135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper memory resource management while the Snort detection engine is processing ICMP packets. An attacker could exploit this vulnerability by sending a series of ICMP packets through an affected device. A successful exploit could allow the attacker to exhaust resources on the affected device, causing the device to reload. **CVE ID : CVE-2021-40114**		
webex_meetings					
Cross-Site Request Forgery (CSRF)	21-Oct-21	5.8	A vulnerability in the application integration feature of Cisco Webex Software could allow an unauthenticated, remote attacker to authorize an external application to integrate with and access a user's account without that user's express consent. This vulnerability is due to improper validation of cross-site request forgery (CSRF) tokens. An attacker could exploit this vulnerability by convincing a targeted user who is currently authenticated to Cisco Webex Software to follow a link designed to pass malicious input to the Cisco Webex Software application authorization interface. A successful exploit could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-2FmKd7T	A-CIS-WEBE-031121/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause Cisco Webex Software to authorize an application on the user's behalf without the express consent of the user, possibly allowing external applications to read data from that user's profile. **CVE ID : CVE-2021-34743**		
cloudfoundry					
capi-release					
Uncontrolled Resource Consumption	27-Oct-21	5	Cloud Controller versions prior to 1.118.0 are vulnerable to unauthenticated denial of Service(DoS) vulnerability allowing unauthenticated attackers to cause denial of service by using REST HTTP requests with label_selectors on multiple V3 endpoints by generating an enormous SQL query. **CVE ID : CVE-2021-22101**	https://www.cloudfoundry.org/blog/cve-2021-22101-cloud-controller-is-vulnerable-to-unauthenticated-denial-of-service/	A-CLO-CAPI-031121/137
cf-deployment					
Uncontrolled Resource Consumption	27-Oct-21	5	Cloud Controller versions prior to 1.118.0 are vulnerable to unauthenticated denial of Service(DoS) vulnerability allowing unauthenticated attackers to cause denial of service by using REST HTTP requests with label_selectors on multiple V3 endpoints by generating an enormous SQL query. **CVE ID : CVE-2021-22101**	https://www.cloudfoundry.org/blog/cve-2021-22101-cloud-controller-is-vulnerable-to-unauthenticated-denial-of-service/	A-CLO-CF-D-031121/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Codesys					
codesys					
Out-of-bounds Write	26-Oct-21	5	Crafted web server requests may cause a heap-based buffer overflow and could therefore trigger a denial-of-service condition due to a crash in the CODESYS V2 web server prior to V1.1.9.22. **CVE ID : CVE-2021-34583**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16876&token=a3f1d937f95e7034879f4f2ea8e5a99b168256a7&download=	A-COD-CODE-031121/139
Buffer Over-read	26-Oct-21	6.4	Crafted web server requests can be utilised to read partial stack or heap memory or may trigger a denial-of- service condition due to a crash in the CODESYS V2 web server prior to V1.1.9.22. **CVE ID : CVE-2021-34584**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16876&token=a3f1d937f95e7034879f4f2ea8e5a99b168256a7&download=	A-COD-CODE-031121/140
Improper Check for Unusual or Exceptional Conditions	26-Oct-21	5	In the CODESYS V2 web server prior to V1.1.9.22 crafted web server requests can trigger a parser error. Since the parser result is not checked under all conditions, a pointer dereference with an invalid address can occur. This leads to a denial of service situation. **CVE ID : CVE-2021-34585**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16876&token=a3f1d937f95e7034879f4f2ea8e5a99b168256a7&download=	A-COD-CODE-031121/141
NULL Pointer Dereference	26-Oct-21	5	In the CODESYS V2 web server prior to V1.1.9.22 crafted web server requests	https://customers.codesys.com/index.p	A-COD-CODE-031121/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may cause a Null pointer dereference in the CODESYS web server and may result in a denial-of-service condition. **CVE ID : CVE-2021-34586**	hp?eID=dumpFile&t=f&f=16876&token=a3f1d937f95e7034879f4f2ea8e5a99b168256a7&download=	
plcwinnt					
Improper Handling of Exceptional Conditions	26-Oct-21	5	In CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56 unauthenticated crafted invalid requests may result in several denial-of-service conditions. Running PLC programs may be stopped, memory may be leaked, or further communication clients may be blocked from accessing the PLC. **CVE ID : CVE-2021-34593**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16877&token=8faab0fc1e069f4edfca5d5aba8146139f67a175&download=	A-COD-PLCW-031121/143
Use of Out-of-range Pointer Offset	26-Oct-21	5.5	A crafted request with invalid offsets may cause an out-of-bounds read or write access in CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56, resulting in a denial-of-service condition or local memory overwrite. **CVE ID : CVE-2021-34595**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16878&token=e5644ec405590e66aefa62304cb8632df9fc9e9c&download=	A-COD-PLCW-031121/144
Access of Uninitialized Pointer	26-Oct-21	4	A crafted request may cause a read access to an uninitialized pointer in CODESYS V2 Runtime Toolkit 32 Bit full and	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=	A-COD-PLCW-031121/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PLCWinNT prior to versions V2.4.7.56, resulting in a denial-of-service condition. **CVE ID : CVE-2021-34596**	16878&token=e5644ec405590e66aefa62304cb8632df9fc9e9c&download=	
runtime_toolkit					
Improper Handling of Exceptional Conditions	26-Oct-21	5	In CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56 unauthenticated crafted invalid requests may result in several denial-of-service conditions. Running PLC programs may be stopped, memory may be leaked, or further communication clients may be blocked from accessing the PLC. **CVE ID : CVE-2021-34593**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16877&token=8faab0fc1e069f4edfca5d5aba8146139f67a175&download=	A-COD-RUNT-031121/146
Use of Out-of-range Pointer Offset	26-Oct-21	5.5	A crafted request with invalid offsets may cause an out-of-bounds read or write access in CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56, resulting in a denial-of-service condition or local memory overwrite. **CVE ID : CVE-2021-34595**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16878&token=e5644ec405590e66aefa62304cb8632df9fc9e9c&download=	A-COD-RUNT-031121/147
Access of Uninitialized Pointer	26-Oct-21	4	A crafted request may cause a read access to an uninitialized pointer in CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56, resulting in a	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16878&token=e5644ec4	A-COD-RUNT-031121/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial-of-service condition. **CVE ID : CVE-2021-34596**	05590e66aefa62304cb8632df9fc9e9c&download=	
Combodo					
itop					
Server-Side Request Forgery (SSRF)	19-Oct-21	5	iTop is an open source web based IT Service Management tool. In affected versions an attacker can call the system setup without authentication. Given specific parameters this can lead to SSRF. This issue has been resolved in versions 2.6.5 and 2.7.5 and later **CVE ID : CVE-2021-32663**	https://github.com/Combodo/iTop/security/advisories/GHSA-ghqc-r8f6-q9m9, https://github.com/Combodo/iTop/commit/43daa2ef088bf928a2386fa19324628c3f19b807, https://github.com/Combodo/iTop/commit/6be9a87c150978752bc68baae1a5c4833ddadfec	A-COM-ITOP-031121/149
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	Combodo iTop is an open source web based IT Service Management tool. In affected versions there is a XSS vulnerability on "run query" page when logged as administrator. This has been resolved in versions 2.6.5 and 2.7.5. **CVE ID : CVE-2021-32664**	https://github.com/Combodo/iTop/security/advisories/GHSA-j758-ggwg-9mpj, https://github.com/Combodo/iTop/commit/86f64	A-COM-ITOP-031121/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				9affc12b5078efc86d9439d67d98f4cb2f6, https://github.com/Combodo/iTop/commit/84741c19f0af6fa8e7082a8807eb089182e7b88a	
content_staging_project					
content_staging					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	3.5	The Content Staging WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and escaping via several parameters that are echo'd out via the ~/templates/settings.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 2.0.1. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. **CVE ID : CVE-2021-39356**	N/A	A-CON-CONT-031121/151
cookie-bar_project					
cookie-bar					
Improper Neutralizatio	25-Oct-21	3.5	The Cookie Bar WordPress plugin through 1.8.8 doesn't	N/A	A-COO-COOK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			properly sanitise the Cookie Bar Message setting, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24653**		031121/152
csdn					
csdn_app					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-21	4.3	Cross-Site Scripting (XSS) vulnerability exists in Csdn APP 4.10.0, which can be exploited by attackers to obtain sensitive information such as user cookies. **CVE ID : CVE-2021-41747**	N/A	A-CSD-CSDN-031121/153
customer_relationship_management_system_project					
customer_relationship_management_system					
Unrestricted Upload of File with Dangerous Type	27-Oct-21	6.5	A file upload vulnerability exists in Sourcecodester Customer Relationship Management System 1.0 via the account update option & customer create option, which could let a remote malicious user upload an arbitrary php file. . **CVE ID : CVE-2021-37221**	N/A	A-CUS-CUST-031121/154
dearhive					
dearflip					
Improper Neutralization of Input During Web Page	18-Oct-21	3.5	The PDF Flipbook, 3D Flipbook WordPress â€“ DearFlip WordPress plugin before 1.7.10 does not escape the class attribute of	N/A	A-DEA-DEAR-031121/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			its shortcode before outputting it back in an attribute, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2021-24732**		
devolutions					
remote_desktop_manager					
Incorrect Default Permissions	18-Oct-21	6.5	An incomplete permission check on entries in Devolutions Remote Desktop Manager before 2021.2.16 allows attackers to bypass permissions via batch custom PowerShell. **CVE ID : CVE-2021-42098**	https://devolutions.net, https://devolutions.net/security/advisories/DEVO-2021-0006	A-DEV-REMO-031121/156
discourse					
discourse					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Oct-21	7.5	Discourse is an open source platform for community discussion. In affected versions maliciously crafted requests could lead to remote code execution. This resulted from a lack of validation in subscribe_url values. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. To workaround the issue without updating, requests with a path starting /webhooks/aws path could be blocked at an upstream proxy. **CVE ID : CVE-2021-41163**	https://github.com/discourse/discourse/security/advisories/GHSA-jcjx-pvpc-qgwq, https://github.com/discourse/discourse/commit/fa3c46cf079d28b086fe1025349bb00223a5d5e9	A-DIS-DISC-031121/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
discourse_reactions					
Exposure of Resource to Wrong Sphere	19-Oct-21	5	Discourse-reactions is a plugin for the Discourse platform that allows user to add their reactions to the post. In affected versions reactions given by user to secure topics and private messages are visible. This issue is patched in version 0.2 of discourse-reaction. Users who are unable to update are advised to disable the Discourse-reactions plugin in admin panel. **CVE ID : CVE-2021-41140**	https://github.com/discourse/discourse-reactions/commit/213d90b82fd15c4186ebc290fee18817d9727d0d, https://github.com/discourse/discourse-reactions/security/advisories/GHSA-9358-hwg5-jrmh	A-DIS-DISC-031121/158
dotnetfoundation					
piranha_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-21	3.5	In PiranhaCMS, versions 7.0.0 to 9.1.1 are vulnerable to stored XSS due to the page title improperly sanitized. By creating a page with a specially crafted page title, a low privileged user can trigger arbitrary JavaScript execution. **CVE ID : CVE-2021-25977**	https://github.com/PiranhaCMS/piranha.core/commit/543bc53c7dbd28c793ec960b57fb0e716c6b18d7	A-DOT-PIRA-031121/159
easy_media_download_project					
easy_media_download					
Improper Neutralization of Input During Web	25-Oct-21	3.5	The Easy Media Download WordPress plugin before 1.1.7 does not escape the text argument of its	N/A	A-EAS-EASY-031121/160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			shortcode, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2021-24699**		
Eclipse					
openj9					
N/A	25-Oct-21	7.5	In Eclipse Openj9 before version 0.29.0, the JVM does not throw IllegalAccessError for MethodHandles that invoke inaccessible interface methods. **CVE ID : CVE-2021-41035**	https://github.com/eclipse-openj9/openj9/pull/13740, https://gitlab.eclipse.org/eclipsefdn/emo-team/emo/-/issues/104, https://bugs.eclipse.org/bugs/show_bug.cgi?id=576395	A-ECL-OPEN-031121/161
elabftw					
elabftw					
Improper Restriction of Excessive Authentication Attempts	22-Oct-21	4	eLabFTW is an open source electronic lab notebook manager for research teams. In versions of eLabFTW before 4.1.0, it allows attackers to bypass a brute-force protection mechanism by using many different forged PHPSESSID values in HTTP Cookie header. This issue has been addressed by implementing brute force	https://github.com/elabftw/elabftw/security/advisories/GHSA-q67h-5pc3-g6jv, https://github.com/elabftw/elabftw/commit/8e92afeec4c3a68	A-ELA-ELAB-031121/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			login protection, as recommended by Owasp with Device Cookies. This mechanism will not impact users and will effectively thwart any brute-force attempts at guessing passwords. The only correct way to address this is to upgrade to version 4.1.0. Adding rate limitation upstream of the eLabFTW service is of course a valid option, with or without upgrading. **CVE ID : CVE-2021-41171**	dc88333881b7e6307f425706b	
emarketdesign					
customer_service_software_\\&_support_ticket_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	The Customer Service Software & Support Ticket System WordPress plugin before 5.10.4 does not sanitize or escape form fields before outputting it in the List, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24622**	N/A	A-EMA-CUST-031121/163
request_a_quote					
Improper Neutralization of Input During Web Page Generation ('Cross-site	25-Oct-21	3.5	The Request a Quote WordPress plugin before 2.3.5 does not sanitise, validate or escape some of its settings in the admin dashboard, leading to authenticated Stored Cross-	N/A	A-EMA-REQU-031121/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Site Scripting issues even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24489**		
Enalean					
tuleap					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Oct-21	6.5	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In affected versions an attacker with read access to a "SVN core" repository could execute arbitrary SQL queries. The following versions contain the fix: Tuleap Community Edition 11.17.99.144, Tuleap Enterprise Edition 11.17-5, Tuleap Enterprise Edition 11.16-7. **CVE ID : CVE-2021-41154**	https://tuleap.net/plugins/tracker/?aid=16213, https://github.com/Enalean/tuleap/commit/ab12b686ced4cf233d3b15b08da008e0553eb6a6, https://github.com/Enalean/tuleap/security/advisories/GHSA-6462-gfv9-jf83	A-ENA-TULE-031121/165
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Oct-21	6.5	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In affected versions Tuleap does not sanitize properly user inputs when constructing the SQL query to browse and search revisions in the CVS repositories. The following versions contain the fix: Tuleap Community Edition 11.17.99.146, Tuleap	https://github.com/Enalean/tuleap/commit/ff75f2899c60a4546ee2d532e68a3febd07bdd14, https://tuleap.net/plugins/git/tuleap/tuleap/stable?a=commit&h=ff75f2899	A-ENA-TULE-031121/166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition 11.17-5, Tuleap Enterprise Edition 11.16-7. **CVE ID : CVE-2021-41155**	c60a4546ee2d532e68a3febd07bdd14, https://tuleap.net/plugins/tracker/?aid=16214	
ethereum					
go_ethereum					
N/A	26-Oct-21	3.5	Go Ethereum is the official Golang implementation of the Ethereum protocol. Prior to version 1.10.9, a vulnerable node is susceptible to crash when processing a maliciously crafted message from a peer. Version v1.10.9 contains patches to the vulnerability. There are no known workarounds aside from upgrading. **CVE ID : CVE-2021-41173**	https://github.com/ethereum/go-ethereum/pull/23801, https://github.com/ethereum/go-ethereum/security/advisories/GHSA-59hh-656j-3p7v, https://github.com/ethereum/go-ethereum/commit/e40b37718326b8b4873b3b00a0db2e6c6d9ea738	A-ETH-GO_E-031121/167
evm_project					
evm					
Always-Incorrect Control Flow Implementation	18-Oct-21	7.5	The evm crate is a pure Rust implementation of Ethereum Virtual Machine. In `evm` crate `< 0.31.0`, `JUMPI` opcode's condition is checked after the destination	https://github.com/rust-blockchain/evm/pull/67, https://github.com/rust-	A-EVM-EVM-031121/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validity check. However, according to Geth and OpenEthereum, the condition check should happen before the destination validity check. This is a **high** severity security advisory if you use `evm` crate for Ethereum mainnet. In this case, you should update your library dependency immediately to on or after `0.31.0`. This is a **low** severity security advisory if you use `evm` crate in Frontier or in a standalone blockchain, because there's no security exploit possible with this advisory. It is **not** recommended to update to on or after `0.31.0` until all the normal chain upgrade preparations have been done. If you use Frontier or other `pallet-evm` based Substrate blockchain, please ensure to update your `spec_version` before updating this. For other blockchains, please make sure to follow a hard-fork process before you update this. **CVE ID : CVE-2021-41153**	blockchain/evm/security/advisories/GHSA-pvh2-pj76-4m96	
Fatek					
winproladder					
Out-of-bounds Write	18-Oct-21	6.8	FATEK Automation WinProladder versions 3.30 and prior lacks proper	N/A	A-FAT-WINP-031121/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied data when parsing project files, which could result in an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2021-38426**		
Stack-based Buffer Overflow	18-Oct-21	6.8	FATEK Automation WinProladder versions 3.30 and prior proper validation of user-supplied data when parsing project files, which could result in a stack-based buffer overflow. An attacker could leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2021-38430**	N/A	A-FAT-WINP-031121/170
Unexpected Sign Extension	18-Oct-21	6.8	FATEK Automation WinProladder versions 3.30 and prior lacks proper validation of user-supplied data when parsing project files, which could result in an unexpected sign extension. An attacker could leverage this vulnerability to execute arbitrary code. **CVE ID : CVE-2021-38434**	N/A	A-FAT-WINP-031121/171
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Oct-21	6.8	FATEK Automation WinProladder versions 3.30 and prior lacks proper validation of user-supplied data when parsing project files, which could result in a memory-corruption condition. An attacker could leverage this vulnerability to	N/A	A-FAT-WINP-031121/172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code in the context of the current process. **CVE ID : CVE-2021-38436**		
Use After Free	18-Oct-21	6.8	A use after free vulnerability in FATEK Automation WinProladder versions 3.30 and prior may be exploited when a valid user opens a malformed project file, which may allow arbitrary code execution. **CVE ID : CVE-2021-38438**	N/A	A-FAT-WINP-031121/173
Out-of-bounds Read	18-Oct-21	4.3	FATEK Automation WinProladder versions 3.30 and prior is vulnerable to an out-of-bounds read, which may allow an attacker to read unauthorized information. **CVE ID : CVE-2021-38440**	N/A	A-FAT-WINP-031121/174
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Oct-21	6.8	FATEK Automation WinProladder versions 3.30 and prior lacks proper validation of user-supplied data when parsing project files, which could result in a heap-corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2021-38442**	N/A	A-FAT-WINP-031121/175
find_my_blocks_project					
find_my_blocks					
Missing Authorization	18-Oct-21	5	The Find My Blocks WordPress plugin before 3.4.0 does not have	N/A	A-FIN-FIND-031121/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorisation checks in its REST API, which could allow unauthenticated users to enumerate private posts' titles. **CVE ID : CVE-2021-24677**		
firefly-iii					
firefly_iii					
Unrestricted Upload of File with Dangerous Type	19-Oct-21	6.5	firefly-iii is vulnerable to Unrestricted Upload of File with Dangerous Type **CVE ID : CVE-2021-3846**	https://hunt r.dev/bounti es/5267ec1c -d204-40d2- bd4f- 6c2dd495ee 18, https://githu b.com/firefly -iii/firefly- iii/commit/a 85b6420c19 ace35134f89 6e094e1971 d8c7954b	A-FIR-FIRE-031121/177
URL Redirection to Untrusted Site ('Open Redirect')	19-Oct-21	4.9	firefly-iii is vulnerable to URL Redirection to Untrusted Site **CVE ID : CVE-2021-3851**	https://githu b.com/firefly -iii/firefly- iii/commit/8 662dfa4c0f7 1efef61c31d c015c6f723d b8318d, https://hunt r.dev/bounti es/549a104 0-9b5e- 420b-9b80- 20700dd9d5 92	A-FIR-FIRE-031121/178
Cross-Site	27-Oct-21	4.3	firefly-iii is vulnerable to	https://githu	A-FIR-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-3900**	b.com/firefly-iii/firefly-iii/commit/c2c8c42ef3194d1aeba8c48240fe2e9063f77635, https://huntr.dev/bounties/909e55b6-ef02-4143-92e4-bc3e8397db76	031121/179
freerdp					
freerdp					
Out-of-bounds Write	21-Oct-21	6.8	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. All FreeRDP clients prior to version 2.4.1 using gateway connections (`/gt:rpc`) fail to validate input data. A malicious gateway might allow client memory to be written out of bounds. This issue has been resolved in version 2.4.1. If you are unable to update then use `/gt:http` rather than /gt:rdp connections if possible or use a direct connection without a gateway. **CVE ID : CVE-2021-41159**	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-vh34-m9h7-95xq	A-FRE-FREE-031121/180
Out-of-bounds Write	21-Oct-21	2.1	FreeRDP is a free implementation of the Remote Desktop Protocol	https://github.com/FreeRDP/FreeRDP	A-FRE-FREE-031121/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(RDP), released under the Apache license. In affected versions a malicious server might trigger out of bound writes in a connected client. Connections using GDI or SurfaceCommands to send graphics updates to the client might send `0` width/height or out of bound rectangles to trigger out of bound writes. With `0` width or heigth the memory allocation will be `0` but the missing bounds checks allow writing to the pointer at this (not allocated) region. This issue has been patched in FreeRDP 2.4.1. **CVE ID : CVE-2021-41160**	/security/advisories/GHSA-7c9r-6r2q-93qg	
Freeswitch					
freeswitch					
N/A	25-Oct-21	5	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. When handling SRTP calls, FreeSWITCH prior to version 1.10.7 is susceptible to a DoS where calls can be terminated by remote attackers. This attack can be done continuously, thus denying encrypted calls during the attack. When a media port that is handling	https://github.com/signalwire/freeswitch/security/advisories/GHSA-jh42-prph-gp36	A-FRE-FREE-031121/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRTP traffic is flooded with a specially crafted SRTP packet, the call is terminated leading to denial of service. This issue was reproduced when using the SDES key exchange mechanism in a SIP environment as well as when using the DTLS key exchange mechanism in a WebRTC environment. The call disconnection occurs due to line 6331 in the source file `switch_rtp.c`, which disconnects the call when the total number of SRTP errors reach a hard-coded threshold (100). By abusing this vulnerability, an attacker is able to disconnect any ongoing calls that are using SRTP. The attack does not require authentication or any special foothold in the caller's or the callee's network. This issue is patched in version 1.10.7. **CVE ID : CVE-2021-41105**		
Uncontrolled Resource Consumption	25-Oct-21	5	Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. FreeSWITCH prior to version 1.10.7 is susceptible to Denial of Service via SIP flooding. When flooding FreeSWITCH with SIP	https://github.com/signalwire/freeswitch/security/advisories/GHSA-jvpq-23v4-gp3m	A-FRE-FREE-031121/183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages, it was observed that after a number of seconds the process was killed by the operating system due to memory exhaustion. By abusing this vulnerability, an attacker is able to crash any FreeSWITCH instance by flooding it with SIP messages, leading to Denial of Service. The attack does not require authentication and can be carried out over UDP, TCP or TLS. This issue was patched in version 1.10.7. **CVE ID : CVE-2021-41145**		
Improper Authentication	26-Oct-21	5	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. By default, SIP requests of the type SUBSCRIBE are not authenticated in the affected versions of FreeSWITCH. Abuse of this security issue allows attackers to subscribe to user agent event notifications without the need to authenticate. This abuse poses privacy concerns and might lead to social engineering or similar attacks. For example, attackers may be able to	https://github.com/signalwire/freeswitch/security/advisories/GHSA-g7xg-7c54-rmpj, https://github.com/signalwire/freeswitch/commit/b21dd4e7f3a6f1d5f7be3ea500a319a5bc11db9e	A-FRE-FREE-031121/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			monitor the status of target SIP extensions. Although this issue was fixed in version v1.10.6, installations upgraded to the fixed version of FreeSWITCH from an older version, may still be vulnerable if the configuration is not updated accordingly. Software upgrades do not update the configuration by default. SIP SUBSCRIBE messages should be authenticated by default so that FreeSWITCH administrators do not need to explicitly set the `auth-subscriptions` parameter. When following such a recommendation, a new parameter can be introduced to explicitly disable authentication. **CVE ID : CVE-2021-41157**		
Exposure of Sensitive Information to an Unauthorized Actor	26-Oct-21	5	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.10.7, an attacker can perform a SIP digest leak attack against FreeSWITCH and receive the challenge response of a gateway configured on the FreeSWITCH server. This is done by challenging	https://github.com/signalwire/freeswitch/security/advisories/GHSA-3v3f-99mv-qvj4, http://seclists.org/fulldisclosure/2021/Oct/40	A-FRE-FREE-031121/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FreeSWITCH's SIP requests with the realm set to that of the gateway, thus forcing FreeSWITCH to respond with the challenge response which is based on the password of that targeted gateway. Abuse of this vulnerability allows attackers to potentially recover gateway passwords by performing a fast offline password cracking attack on the challenge response. The attacker does not require special network privileges, such as the ability to sniff the FreeSWITCH's network traffic, to exploit this issue. Instead, what is required for this attack to work is the ability to cause the victim server to send SIP request messages to the malicious party. Additionally, to exploit this issue, the attacker needs to specify the correct realm which might in some cases be considered secret. However, because many gateways are actually public, this information can easily be retrieved. The vulnerability appears to be due to the code which handles challenges in `sofia_reg.c`, `sofia_reg_handle_sip_r_challenge()` which does not check if the challenge is originating from the actual gateway. The		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lack of these checks allows arbitrary UACs (and gateways) to challenge any request sent by FreeSWITCH with the realm of the gateway being targeted. This issue is patched in version 10.10.7. Maintainers recommend that one should create an association between a SIP session for each gateway and its realm to make a check be put into place for this association when responding to challenges. **CVE ID : CVE-2021-41158**		
frentix					
openolat					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-21	4	OpenOlat is a web-based e-learning platform for teaching, learning, assessment and communication, an LMS, a learning management system. In affected versions by manipulating the HTTP request an attacker can modify the path of a requested file download in the folder component to point to anywhere on the target system. The attack could be used to read any file accessible in the web root folder or outside, depending on the configuration of the system and the properly configured permission of the application server user. The	https://jira.openolat.org/browse/OO-5696, https://github.com/OpenOLAT/OpenOLAT/security/advisories/GHSA-m8j5-837g-2p3f, https://github.com/OpenOLAT/OpenOLAT/commit/418bb509ffcb0e25ab4390563c6c47f0458583e	A-FRE-OPEN-031121/186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack requires an OpenOlat user account or the enabled guest user feature together with the usage of the folder component in a course. The attack does not allow writing of arbitrary files, it allows only reading of files and also only ready of files that the attacker knows the exact path which is very unlikely at least for OpenOlat data files. The problem is fixed in version 15.5.8 and 16.0.1 It is advised to upgrade to version 16.0.x. There are no known workarounds to fix this problem, an upgrade is necessary. **CVE ID : CVE-2021-41152**	b	
galette					
galette					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-21	3.5	Galette is a membership management web application geared towards non profit organizations. In versions prior to 0.9.5, malicious javascript code can be stored to be displayed later on self subscription page. The self subscription feature can be disabled as a workaround (this is the default state). Malicious javascript code can be executed (not stored) on login and retrieve password pages. This issue is patched in version 0.9.5.	https://github.com/galette/galette/security/advisories/GHSA-vjc9-mj44-x59q, https://bugs.galette.eu/issues/1535, https://github.com/galette/galette/commit/514418da973ae5b84bf97f94bd288a41e8e3f	A-GAL-GALE-031121/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21319	0a6	
game-server-status_project					
game-server-status					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-21	6.5	The Game Server Status WordPress plugin through 1.0 does not validate or escape the server_id parameter before using it in SQL statement, leading to an Authenticated SQL Injection in an admin page **CVE ID : CVE-2021-24662**	N/A	A-GAM-GAME-031121/188
gamepress_project					
gamepress					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	4.3	The GamePress WordPress plugin through 1.1.0 does not escape the op_edit POST parameter before outputting it back in multiple Game Option pages, leading to Reflected Cross-Site Scripting issues **CVE ID : CVE-2021-24617**	N/A	A-GAM-GAME-031121/189
gestionaleopen					
gestionale_open					
Incorrect Default Permissions	26-Oct-21	9.3	An Insecure Permissions issue exists in Gestionale Open 11.00.00. A low privilege account is able to rename the mysqld.exe file located in bin folder and replace with a malicious file that would connect back to an attacking computer giving system level privileges (nt authority\system) due to the service running as Local	N/A	A-GES-GEST-031121/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			System. While a low privilege user is unable to restart the service through the application, a restart of the computer triggers the execution of the malicious file. The application also have unquoted service path issues. **CVE ID : CVE-2021-37363**		
getgrav					
grav					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	grav is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3904**	https://huntr.dev/bounties/b1182515-d911-4da9-b4f7-b4c341a62a8d, https://github.com/getgrav/grav/commit/afc69a3229bb6fe120b2c1ea27bc6f196ed7284d	A-GET-GRAV-031121/191
gjson_project					
gjson					
Incorrect Comparison	22-Oct-21	5	GJSON before 1.9.3 allows a ReDoS (regular expression denial of service) attack. **CVE ID : CVE-2021-42836**	https://github.com/tidwall/gjson/commit/77a57fda87dca6d0d7d4627d512a630f89a91c96, https://github.com/tidwal	A-GJS-GJSO-031121/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				l/gjson/issues/237, https://github.com/tidwall/gjson/commit/590010fdac311cc8990ef5c97448d4fec8f29944	
glasswire					
glasswire					
Improper Control of Generation of Code ('Code Injection')	18-Oct-21	7.5	A code injection vulnerability exists within the firewall software of GlassWire v2.1.167 that could lead to arbitrary code execution from a file in the user path on first execution. **CVE ID : CVE-2021-22961**	N/A	A-GLA-GLAS-031121/193
GNU					
mailman					
Improper Restriction of Excessive Authentication Attempts	21-Oct-21	6.8	GNU Mailman before 2.1.35 may allow remote Privilege Escalation. A certain csrf_token value is derived from the admin password, and may be useful in conducting a brute-force attack against that password. **CVE ID : CVE-2021-42096**	https://mail.python.org/archives/list/mailman-announce@python.org/thread/IKCO6JU755AP5G5TKMBJL6IEZQTTNPDQ/, https://bugs.launchpad.net/mailman/+bug/1947639, http://www.openwall.com/lists/oss-	A-GNU-MAIL-031121/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				security/2021/10/21/4	
Cross-Site Request Forgery (CSRF)	21-Oct-21	9.3	GNU Mailman before 2.1.35 may allow remote Privilege Escalation. A csrf_token value is not specific to a single user account. An attacker can obtain a value within the context of an unprivileged user account, and then use that value in a CSRF attack against an admin (e.g., for account takeover). **CVE ID : CVE-2021-42097**	https://mail.python.org/archives/list/mailman-announce@python.org/thread/IKCO6JU755AP5G5TKMBJL6IEZQTTNPDQ/, https://bugs.launchpad.net/mailman/+bug/1947640, http://www.openwall.com/lists/oss-security/2021/10/21/4	A-GNU-MAIL-031121/195
Golang					
go					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Oct-21	7.5	Go before 1.16.9 and 1.17.x before 1.17.2 has a Buffer Overflow via large arguments in a function invocation from a WASM module, when GOARCH=wasm GOOS=js is used. **CVE ID : CVE-2021-38297**	https://groups.google.com/g/golang-announce/c/AEBu9j7yj5A	A-GOL-GO-031121/196
gonitro					
nitro_pro					
Use After Free	18-Oct-21	6.8	An exploitable use-after-free vulnerability exists in the JavaScript implementation of	N/A	A-GON-NITR-031121/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nitro Pro PDF. A specially crafted document can cause an object containing the path to a document to be destroyed and then later reused, resulting in a use-after-free vulnerability, which can lead to code execution under the context of the application. An attacker can convince a user to open a document to trigger this vulnerability. **CVE ID : CVE-2021-21796**		
Double Free	18-Oct-21	6.8	An exploitable double-free vulnerability exists in the JavaScript implementation of Nitro Pro PDF. A specially crafted document can cause a reference to a timeout object to be stored in two different places. When closed, the document will result in the reference being released twice. This can lead to code execution under the context of the application. An attacker can convince a user to open a document to trigger this vulnerability. **CVE ID : CVE-2021-21797**	N/A	A-GON-NITR-031121/198
great-quotes_project					
great-quotes					
Improper Neutralization of Input During Web Page Generation	25-Oct-21	3.5	The Great Quotes WordPress plugin through 1.0.0 does not sanitise and escape the Quote and Author fields of its Quotes, which could allow high privilege users to	N/A	A-GRE-GREA-031121/199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed. **CVE ID : CVE-2021-24785**		
gridprosoftware					
request_management					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-21	7.5	Gridpro Request Management for Windows Azure Pack before 2.0.7912 allows Directory Traversal for remote code execution, as demonstrated by ..\\ in a scriptName JSON value to ServiceManagerTenant/GetVisibilityMap. **CVE ID : CVE-2021-40371**	https://www.gridprosoftware.com/products/requestmanagement/	A-GRI-REQU-031121/200
hcltechsw					
connections					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	3.5	"HCL Connections Security Update for Reflected Cross-Site Scripting (XSS) Vulnerability" **CVE ID : CVE-2021-27746**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0094194	A-HCL-CONN-031121/201
heateor					
sassy_social_share					
Deserialization of Untrusted Data	21-Oct-21	6.5	Version 3.3.23 of the Sassy Social Share WordPress plugin is vulnerable to PHP Object Injection via the wp_ajax_heateor_sss_import_config AJAX action due to deserialization of unvalidated user supplied	https://plugins.trac.wordpress.org/changeset/2600464/sassy-social-share/trunk/admin/class-	A-HEA-SASS-031121/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inputs via the import_config function found in the ~/admin/class-sassy-social-share-admin.php file. This can be exploited by underprivileged authenticated users due to a missing capability check on the import_config function. **CVE ID : CVE-2021-39321**	sassy-social-share-admin.php	
Huawei					
emui					
N/A	28-Oct-21	5	There is a DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause DoS attacks. **CVE ID : CVE-2021-22402**	https://consumer.huawei.com/en/support/bulletin/2021/7/	A-HUA-EMUI-031121/203
magic_ui					
N/A	28-Oct-21	5	There is a DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause DoS attacks. **CVE ID : CVE-2021-22402**	https://consumer.huawei.com/en/support/bulletin/2021/7/	A-HUA-MAGI-031121/204
manageone					
Improper Neutralization of Formula Elements in a CSV File	27-Oct-21	6	There is a CSV injection vulnerability in ManageOne, iManager NetEco and iManager NetEco 6000. An attacker with high privilege may exploit this vulnerability through some operations to inject the CSV files. Due to insufficient input validation of some	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-csv-en	A-HUA-MANA-031121/205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameters, the attacker can exploit this vulnerability to inject CSV files to the target device. **CVE ID : CVE-2021-37131**		
pcmanager					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Oct-21	3.3	There is a path traversal vulnerability in Huawei PC product. Because the product does not filter path with special characters,attackers can construct a file path with special characters to exploit this vulnerability. Successful exploitation could allow the attacker to transport a file to certain path.Affected product versions include:PC Smart Full Scene 11.1 versions PCManager 11.1.1.97. **CVE ID : CVE-2021-37124**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211008-01-share-en	A-HUA-PCMA-031121/206
pc_smart_full_scene					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Oct-21	3.3	There is a path traversal vulnerability in Huawei PC product. Because the product does not filter path with special characters,attackers can construct a file path with special characters to exploit this vulnerability. Successful exploitation could allow the attacker to transport a file to certain path.Affected product versions include:PC Smart Full Scene 11.1 versions PCManager	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211008-01-share-en	A-HUA-PC_S-031121/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.1.1.97. **CVE ID : CVE-2021-37124**		
IBM					
business_automation_workflow					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-21	4.3	IBM Business Automation Workflow 18.0, 19.0, 20.0, and 21.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204833. **CVE ID : CVE-2021-29835**	https://www.ibm.com/support/pages/node/6507319, https://exchange.xforce.ibmcloud.com/vulnerabilities/204833	A-IBM-BUSI-031121/208
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	IBM Business Automation Workflow 18.0, 19.0, 20.0, and 21.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 206581. **CVE ID : CVE-2021-29878**	https://exchange.xforce.ibmcloud.com/vulnerabilities/206581, https://www.ibm.com/support/pages/node/6501949	A-IBM-BUSI-031121/209
engineering_lifecycle_optimization					
Improper Neutralization of Input During Web Page	27-Oct-21	3.5	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript	https://exchange.xforce.ibmcloud.com/vulnerabilities/199482,	A-IBM-ENGI-031121/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199482. **CVE ID : CVE-2021-29673**	https://www.ibm.com/support/pages/node/6508583	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **CVE ID : CVE-2021-29713**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200967, https://www.ibm.com/support/pages/node/6508583	A-IBM-ENGI-031121/211
Improper Privilege Management	27-Oct-21	6	IBM Jazz Team Server products could allow an authenticated user to obtain elevated privileges under certain configurations. IBM X-Force ID: 203025. **CVE ID : CVE-2021-29774**	https://exchange.xforce.ibmcloud.com/vulnerabilities/203025, https://www.ibm.com/support/pages/node/6508583	A-IBM-ENGI-031121/212
engineering_workflow_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially	https://exchange.xforce.ibmcloud.com/vulnerabilities/199482, https://www.ibm.com/support/page	A-IBM-ENGI-031121/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to credentials disclosure within a trusted session. IBM X-Force ID: 199482. **CVE ID : CVE-2021-29673**	s/node/6508583	
Improper Privilege Management	27-Oct-21	6	IBM Jazz Team Server products could allow an authenticated user to obtain elevated privileges under certain configurations. IBM X-Force ID: 203025. **CVE ID : CVE-2021-29774**	https://exchange.xforce.ibmcloud.com/vulnerabilities/203025, https://www.ibm.com/support/pages/node/6508583	A-IBM-ENGI-031121/214
planning_analytics					
Incorrect Permission Assignment for Critical Resource	27-Oct-21	5	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 198755. **CVE ID : CVE-2021-20526**	https://www.ibm.com/support/pages/node/6507095, https://exchange.xforce.ibmcloud.com/vulnerabilities/198755	A-IBM-PLAN-031121/215
qradar_advisor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-21	4.3	IBM QRadar Advisor 2.5 through 2.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID:	https://www.ibm.com/support/pages/node/6506461, https://exchange.xforce.ibmcloud.com/vulnerabilities/209566	A-IBM-QRAD-031121/216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			209566. **CVE ID : CVE-2021-38896**		
rational_collaborative_lifecycle_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199482. **CVE ID : CVE-2021-29673**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199482, https://www.ibm.com/support/pages/node/6508583	A-IBM-RATI-031121/217
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **CVE ID : CVE-2021-29713**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200967, https://www.ibm.com/support/pages/node/6508583	A-IBM-RATI-031121/218
Improper Privilege Management	27-Oct-21	6	IBM Jazz Team Server products could allow an authenticated user to obtain elevated privileges under certain configurations. IBM X-Force ID: 203025. **CVE ID : CVE-2021-29774**	https://exchange.xforce.ibmcloud.com/vulnerabilities/203025, https://www.ibm.com/support/pages/node/6508583	A-IBM-RATI-031121/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rational_doors_next_generation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199482. **CVE ID : CVE-2021-29673**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199482, https://www.ibm.com/support/pages/node/6508583	A-IBM-RATI-031121/220
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **CVE ID : CVE-2021-29713**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200967, https://www.ibm.com/support/pages/node/6508583	A-IBM-RATI-031121/221
Improper Privilege Management	27-Oct-21	6	IBM Jazz Team Server products could allow an authenticated user to obtain elevated privileges under certain configurations. IBM X-Force ID: 203025. **CVE ID : CVE-2021-29774**	https://exchange.xforce.ibmcloud.com/vulnerabilities/203025, https://www.ibm.com/support/pages/node/6508583	A-IBM-RATI-031121/222
rational_engineering_lifecycle_manager					
Improper Neutralizatio	27-Oct-21	3.5	IBM Jazz Team Server products are vulnerable to	https://exchange.xforce.i	A-IBM-RATI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199482. **CVE ID : CVE-2021-29673**	bmcloud.com/vulnerabilities/199482, https://www.ibm.com/support/pages/node/6508583	031121/223
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **CVE ID : CVE-2021-29713**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200967, https://www.ibm.com/support/pages/node/6508583	A-IBM-RATI-031121/224
Improper Privilege Management	27-Oct-21	6	IBM Jazz Team Server products could allow an authenticated user to obtain elevated privileges under certain configurations. IBM X-Force ID: 203025. **CVE ID : CVE-2021-29774**	https://exchange.xforce.ibmcloud.com/vulnerabilities/203025, https://www.ibm.com/support/pages/node/6508583	A-IBM-RATI-031121/225
rational_team_concert					
Improper Neutralization of Input During Web Page	27-Oct-21	3.5	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript	https://exchange.xforce.ibmcloud.com/vulnerabilities/199482,	A-IBM-RATI-031121/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199482. **CVE ID : CVE-2021-29673**	https://www.ibm.com/support/pages/node/6508583	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-21	3.5	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **CVE ID : CVE-2021-29713**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200967, https://www.ibm.com/support/pages/node/6508583	A-IBM-RATI-031121/227
Improper Privilege Management	27-Oct-21	6	IBM Jazz Team Server products could allow an authenticated user to obtain elevated privileges under certain configurations. IBM X-Force ID: 203025. **CVE ID : CVE-2021-29774**	https://exchange.xforce.ibmcloud.com/vulnerabilities/203025, https://www.ibm.com/support/pages/node/6508583	A-IBM-RATI-031121/228
security_risk_manager_on_cp4s					
Cleartext Storage of Sensitive Information	19-Oct-21	4	IBM Security Risk Manager on CP4S 1.7.0.0 stores user credentials in plain clear text which can be read by a an authenticatedl privileged user. IBM X-Force ID: 209940. **CVE ID : CVE-2021-38911**	https://exchange.xforce.ibmcloud.com/vulnerabilities/209940, https://www.ibm.com/support/page	A-IBM-SECU-031121/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				s/node/6505281	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	IBM Security Risk Manager on CP4S 1.7.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 207828. **CVE ID : CVE-2021-29912**	https://exchange.xforce.ibmcloud.com/vulnerabilities/207828, https://www.ibm.com/support/pages/node/6505283	A-IBM-SECU-031121/230
spectrum_virtualize					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force ID: 206229. **CVE ID : CVE-2021-29873**	https://www.ibm.com/support/pages/node/6497111, https://www.ibm.com/support/pages/node/6507091, https://exchange.xforce.ibmcloud.com/vulnerabilities/206229	A-IBM-SPEC-031121/231
spectrum_virtualize_for_public_cloud					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force	https://www.ibm.com/support/pages/node/6497111, https://www.ibm.com/s	A-IBM-SPEC-031121/232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: 206229. **CVE ID : CVE-2021-29873**	upport/pages/node/6507091, https://exchange.xforce.ibmcloud.com/vulnerabilities/206229	
storwize_v3500_software					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force ID: 206229. **CVE ID : CVE-2021-29873**	https://www.ibm.com/support/pages/node/6497111, https://www.ibm.com/support/pages/node/6507091, https://exchange.xforce.ibmcloud.com/vulnerabilities/206229	A-IBM-STOR-031121/233
storwize_v3700_software					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force ID: 206229. **CVE ID : CVE-2021-29873**	https://www.ibm.com/support/pages/node/6497111, https://www.ibm.com/support/pages/node/6507091, https://exchange.xforce.ibmcloud.com/vulnerabiliti	A-IBM-STOR-031121/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				es/206229	
storwize_v5000_software					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force ID: 206229. **CVE ID : CVE-2021-29873**	https://www.ibm.com/support/pages/node/6497111, https://www.ibm.com/support/pages/node/6507091, https://exchange.xforce.ibmcloud.com/vulnerabilities/206229	A-IBM-STOR-031121/235
storwize_v5100_software					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force ID: 206229. **CVE ID : CVE-2021-29873**	https://www.ibm.com/support/pages/node/6497111, https://www.ibm.com/support/pages/node/6507091, https://exchange.xforce.ibmcloud.com/vulnerabilities/206229	A-IBM-STOR-031121/236
storwize_v7000_software					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a	https://www.ibm.com/support/pages/node/6497111,	A-IBM-STOR-031121/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restricted shell escape vulnerability. IBM X-Force ID: 206229. **CVE ID : CVE-2021-29873**	https://www.ibm.com/support/pages/node/6507091, https://exchange.xforce.ibmcloud.com/vulnerabilities/206229	
transformation_extender_advanced					
Incorrect Authorization	21-Oct-21	4.3	IBM Standards Processing Engine (IBM Transformation Extender Advanced 9.0 and 10.0) does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 207090. **CVE ID : CVE-2021-29883**	https://www.ibm.com/support/pages/node/6507077, https://exchange.xforce.ibmcloud.com/vulnerabilities/207090	A-IBM-TRAN-031121/238
icegram					
icegram					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	WordPress Popups, Welcome Bar, Optins and Lead Generation Plugin – Icegram (versions <= 2.0.2) vulnerable at "Headline" (&message_data[16][headline]) input. **CVE ID : CVE-2021-36832**	https://wordpress.org/plugins/icegram/#developers	A-ICE-ICEG-031121/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
indeed-job-importer_project					
indeed-job-importer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	The Indeed Job Importer WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/indeed-job-importer/trunk/indeed-job-importer.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.0.5. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. **CVE ID : CVE-2021-39355**	N/A	A-IND-INDE-031121/240
interchain					
cosmos_sdk					
Improper Check for Unusual or Exceptional Conditions	20-Oct-21	4	The Cosmos-SDK is a framework for building blockchain applications in Golang. Affected versions of the SDK were vulnerable to a consensus halt due to non-deterministic behaviour in a ValidateBasic method in the x/authz module. The MsgGrant of the x/authz module contains a Grant field which includes a user-defined expiration time for when the authorization	https://forum.cosmos.network/t/cosmos-sdk-vulnerability-retrospective-security-advisory-jackfruit-october-12-2021/5349, https://github.com/cosm	A-INT-COSM-031121/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			grant expires. In Grant.ValidateBasic(), that time is compared to the nodeâ€™s local clock time. Any chain running an affected version of the SDK with the authz module enabled could be halted by anyone with the ability to send transactions on that chain. Recovery would require applying the patch and rolling back the latest block. Users are advised to update to version 0.44.2. **CVE ID : CVE-2021-41135**	os/cosmos-sdk/security/advisories/GHSA-2p6r-37p9-89p2	
ivorysearch					
ivory_search					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	4.3	Reflected Cross-Site Scripting (XSS) vulnerability in WordPress Ivory Search plugin (versions <= 4.6.6). Vulnerable parameter: &post. **CVE ID : CVE-2021-36869**	https://wordpress.org/plugins/add-search-to-menu/#developers	A-IVO-IVOR-031121/242
Jquery					
jquery_ui					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-21	4.3	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField`	https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc, https://github.com/jquery/jquery-ui/pull/1954	A-JQU-JQUE-031121/243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources. **CVE ID : CVE-2021-41182**	/commits/6809ce843e5ac4128108ea4c15cbc100653c2b63, https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-21	4.3	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources. **CVE ID : CVE-2021-41183**	https://bugs.jqueryui.com/ticket/15284, https://github.com/jquery/jquery-ui/pull/1953, https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4, https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/	A-JQU-JQUE-031121/244
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-Oct-21	4.3	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code.	https://github.com/jquery/jquery-ui/commit/effa323f1505f2ce7a324e4f429fa9032c7	A-JQU-JQUE-031121/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources. **CVE ID : CVE-2021-41184**	2f280, https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327, https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/	
jquery-reply-to-comment_project					
jquery-reply-to-comment					
Cross-Site Request Forgery (CSRF)	25-Oct-21	4.3	The jQuery Reply to Comment WordPress plugin through 1.31 does not have any CSRF check when saving its settings, nor sanitise or escape its 'Quote String' and 'Reply String' settings before outputting them in Comments, leading to a Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24543**	N/A	A-JQU-JQUE-031121/246
Juniper					
ctpview					
Cleartext Transmission of Sensitive Information	19-Oct-21	5.8	The Juniper Networks CTPView server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header which allows servers to indicate that content from the requested domain will only be served over HTTPS.	https://kb.juniper.net/JSA11210	A-JUN-CTPV-031121/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The lack of HSTS may leave the system vulnerable to downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. This issue affects Juniper Networks CTPView: 7.3 versions prior to 7.3R7; 9.1 versions prior to 9.1R3. **CVE ID : CVE-2021-0296**		
session_and_resource_control					
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-21	5	An Information Exposure vulnerability in Juniper Networks SRC Series devices configured for NETCONF over SSH permits the negotiation of weak ciphers, which could allow a remote attacker to obtain sensitive information. A remote attacker with read and write access to network data could exploit this vulnerability to display plaintext bits from a block of ciphertext and obtain sensitive information. This issue affects all Juniper Networks SRC Series versions prior to 4.13.0-R6. **CVE ID : CVE-2021-31352**	https://kb.juniper.net/JSA11217	A-JUN-SESS-031121/248
N/A	19-Oct-21	5	A configuration weakness in the JBoss Application Server (AppSvr) component of Juniper Networks SRC Series allows a remote attacker to send a specially crafted query to cause the web server to disclose sensitive	https://kb.juniper.net/JSA11248	A-JUN-SESS-031121/249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information in the HTTP response which allows the attacker to obtain sensitive information. **CVE ID : CVE-2021-31380**		
N/A	19-Oct-21	6.4	A configuration weakness in the JBoss Application Server (AppSvr) component of Juniper Networks SRC Series allows a remote attacker to send a specially crafted query to cause the web server to delete files which may allow the attacker to disrupt the integrity and availability of the system. **CVE ID : CVE-2021-31381**	https://kb.juniper.net/JSA11248	A-JUN-SESS-031121/250
libmobi_project					
libmobi					
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-Oct-21	5.8	libmobi is vulnerable to Use of Out-of-range Pointer Offset **CVE ID : CVE-2021-3888**	https://github.com/bfabiszewski/libmobi/commit/c78e186739b50d156cb3da5d08d70294f0490853, https://huntr.dev/bounties/722b3acb-792b-4429-a98d-bb80efb8938d	A-LIB-LIBM-031121/251
Improper Restriction of Operations within the Bounds of a	19-Oct-21	5.8	libmobi is vulnerable to Use of Out-of-range Pointer Offset **CVE ID : CVE-2021-3889**	https://huntr.dev/bounties/efb3e261-3f7d-4a45-8114-	A-LIB-LIBM-031121/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer				e0ace6b21516, https://github.com/bfabiszewski/libmobi/commit/bec783e6212439a335ba6e8df7ab8ed610ca9a21	
libtpms_project					
libtpms					
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-Oct-21	7.1	A flaw was found in the libtpms code that may cause access beyond the boundary of internal buffers. The vulnerability is triggered by specially-crafted TPM2 command packets that then trigger the issue when the state of the TPM2's volatile state is written. The highest threat from this vulnerability is to system availability. This issue affects libtpms versions before 0.8.5, before 0.7.9 and before 0.6.6. **CVE ID : CVE-2021-3746**	https://bugzilla.redhat.com/show_bug.cgi?id=1998588	A-LIB-LIBT-031121/253
Linuxfoundation					
backstage					
Improper Limitation of a Pathname to a Restricted Directory ('Path	18-Oct-21	4	Backstage is an open platform for building developer portals. In affected versions A malicious actor could read sensitive files from the environment where Scaffolder Tasks are run. The attack is executed	https://github.com/backstage/backstage/security/advisories/GHSA-pvv8-8fx9-h673, https://githu	A-LIN-BACK-031121/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			by crafting a custom Scaffolder template with a `github:publish:pull-request` action and a particular source path. When the template is executed the sensitive files would be included in the published pull request. This vulnerability is mitigated by the fact that an attacker would need access to create and register templates in the Backstage catalog, and that the attack is very visible given that the exfiltration happens via a pull request. The vulnerability is patched in the `0.15.9` release of `@backstage/plugin-scaffolder-backend`. **CVE ID : CVE-2021-41151**	b.com/backstage/backstage/commit/6968962c920508eae19a4c1c200fa2c8980a4006	
the_update_framework					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-21	8.8	python-tuf is a Python reference implementation of The Update Framework (TUF). In both clients (`tuf/client` and `tuf/ngclient`), there is a path traversal vulnerability that in the worst case can overwrite files ending in `.json` anywhere on the client system on a call to `get_one_valid_targetinfo()`. It occurs because the rolename is used to form the filename, and may contain path traversal characters (ie `../../name.json`). The impact	https://github.com/theupdateframework/python-tuf/commit/4ad7ae48fda594b640139c3b7eae21ed5155a102, https://github.com/theupdateframework/python-tuf/security/advisories/GHSA-wjw6-2cqr-j4qr	A-LIN-THE_-031121/255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is mitigated by a few facts: It only affects implementations that allow arbitrary rolename selection for delegated targets metadata, The attack requires the ability to A) insert new metadata for the path-traversing role and B) get the role delegated by an existing targets metadata, The written file content is heavily restricted since it needs to be a valid, signed targets file. The file extension is always .json. A fix is available in version 0.19 or newer. There are no workarounds that do not require code changes. Clients can restrict the allowed character set for rolenames, or they can store metadata in files named in a way that is not vulnerable: neither of these approaches is possible without modifying python-tuf. **CVE ID : CVE-2021-41131**		
mainwp					
mainwp_child_reports					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	18-Oct-21	6.5	The MainWP Child Reports WordPress plugin before 2.0.8 does not validate or sanitise the order parameter before using it in a SQL statement in the admin dashboard, leading to an SQL injection issue	N/A	A-MAI-MAIN-031121/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			**CVE ID : CVE-2021-24754**		
mangboard					
mang_board					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-21	5	A vulnerability was found in Mangboard(WordPress plugin). A SQL-Injection vulnerability was found in order_type parameter. The order_type parameter makes a SQL query using unfiltered data. This vulnerability allows a remote attacker to steal user information. **CVE ID : CVE-2021-26609**	N/A	A-MAN-MANG-031121/257
Mcafee					
epolicy_orchestrator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-21	3.5	Stored Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 11 allows ePO administrators to inject arbitrary web script or HTML via multiple parameters where the administrator's entries were not correctly sanitized. **CVE ID : CVE-2021-31834**	https://kc.mcafee.com/corporate/index?page=content&id=SB10366	A-MCA-EPOL-031121/258
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-21	4.3	Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 11 allows ePO administrators to inject arbitrary web script or HTML via a specific parameter where the administrator's entries were not correctly sanitized. **CVE ID : CVE-2021-31835**	https://kc.mcafee.com/corporate/index?page=content&id=SB10366	A-MCA-EPOL-031121/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
total_protection					
Improper Privilege Management	26-Oct-21	7.2	Privilege escalation vulnerability in the Windows trial installer of McAfee Total Protection (MTP) prior to 16.0.34_x may allow a local user to run arbitrary code as the admin user by replacing a specific temporary file created during the installation of the trial version of MTP. **CVE ID : CVE-2021-23877**	https://service.mcafee.com/webcenter/portal/cp/home/articleview?articleId=TS103215	A-MCA-TOTA-031121/260
microco					
bluemonday					
Improper Input Validation	18-Oct-21	7.5	The bluemonday sanitizer before 1.0.16 for Go, and before 0.0.8 for Python (in pybluemonday), does not properly enforce policies associated with the SELECT, STYLE, and OPTION elements. **CVE ID : CVE-2021-42576**	N/A	A-MIC-BLUE-031121/261
Microweber					
microweber					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	4.3	Cross Site Scripting (XSS). vulnerability exists in Microweber CMS 1.2.7 via the Login form, which could let a malicious user execute Javascript by Inserting code in the request form. **CVE ID : CVE-2021-33988**	N/A	A-MIC-MICR-031121/262
modern-async_project					
modern-async					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	20-Oct-21	5	modern-async is an open source JavaScript tooling library for asynchronous operations using async/await and promises. In affected versions a bug affecting two of the functions in this library: forEachSeries and forEachLimit. They should limit the concurrency of some actions but, in practice, they don't. Any code calling these functions will be written thinking they would limit the concurrency but they won't. This could lead to potential security issues in other projects. The problem has been patched in 1.0.4. There is no workaround. **CVE ID : CVE-2021-41167**	https://github.com/nicolas-van/modern-async/issues/5, https://github.com/nicolas-van/modern-async/commit/0010d28de1b15d51db3976080e26357fa7144436, https://github.com/nicolas-van/modern-async/security/advisories/GHSA-3pcq-34w5-p4g2	A-MOD-MODE-031121/263
motopress					
motopress-slider-lite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-21	3.5	The Responsive WordPress Slider WordPress plugin through 2.2.0 does not sanitise and escape some of the Slider options, allowing Cross-Site Scripting payloads to be set in them. Furthermore, as by default any authenticated user is allowed to create Sliders (https://wordpress.org/support/topic/slider-can-be-changed-from-any-user-even-subscriber/, such	N/A	A-MOT-MOTO-031121/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings can be changed in the plugin's settings), this would allow user with a role as low as subscriber to perform Cross-Site Scripting attacks against logged in admins viewing the slider list and could lead to privilege escalation by creating a rogue admin account for example. **CVE ID : CVE-2021-24544**		
mpl-publisher_project					
mpl-publisher					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	The MPL-Publisher WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/libs/PublisherController.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.30.2. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. **CVE ID : CVE-2021-39343**	N/A	A-MPL-MPL--031121/265
Mybb					
mybb					
Improper Neutralizatio	26-Oct-21	3.5	MyBB before 1.8.28 allows stored XSS because the	https://github.com/mybb	A-MYB-MYBB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			displayed Template Name value in the Admin CP's theme management is not escaped properly. **CVE ID : CVE-2021-41866**	/mybb/security/advisories/GHSA-gxhv-r3m5-6qv7	031121/266
mycodo_project					
mycodo					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Oct-21	4	Mycodo is an environmental monitoring and regulation system. An exploit in versions prior to 8.12.7 allows anyone with access to endpoints to download files outside the intended directory. A patch has been applied and a release made. Users should upgrade to version 8.12.7. As a workaround, users may manually apply the changes from the fix commit. **CVE ID : CVE-2021-41185**	https://github.com/kizniche/Mycodo/security/advisories/GHSA-252r-94ph-m229, https://github.com/kizniche/Mycodo/commit/23ac5dd422029c2b6ae1701a3599b6d41b66a6a9	A-MYC-MYCO-031121/267
myfactory					
fms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	4.3	myfactory.FMS before 7.1-912 allows XSS via the UID parameter. **CVE ID : CVE-2021-42565**	N/A	A-MYF-FMS-031121/268
Improper Neutralization of Input During Web Page	18-Oct-21	4.3	myfactory.FMS before 7.1-912 allows XSS via the Error parameter. **CVE ID : CVE-2021-42566**	N/A	A-MYF-FMS-031121/269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')					
nameko					
nameko					
Deserialization of Untrusted Data	26-Oct-21	6.8	Nameko through 2.13.0 can be tricked into performing arbitrary code execution when deserializing the config file. **CVE ID : CVE-2021-41078**	N/A	A-NAM-NAME-031121/270
Netapp					
e-series_santricity_os_controller					
Incorrect Authorization	20-Oct-21	7.1	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets,	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35550**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35556**		
Incorrect Authorization	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35559**		
N/A	20-Oct-21	5.1	Vulnerability in the Java SE product of Oracle Java SE (component: Deployment). The supported version that is affected is Java SE: 8u301. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments,	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35560**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Utility). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35561**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Keytool). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35564**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35565**		
N/A	20-Oct-21	6.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in Java SE, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-35567**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.c	A-NET-E-SE-031121/279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35578**	om/advisory/ntap-20211022-0004/	
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35586**		
N/A	20-Oct-21	2.6	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u311, 8u301; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-	A-NET-E-SE-031121/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35588**	0004/	
N/A	20-Oct-21	4.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle	https://www.oracle.com/security-	A-NET-E-SE-031121/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35603**	alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	
e-series_santricity_storage_manager					
Incorrect	20-Oct-21	7.1	Vulnerability in the Java SE,	https://ww	A-NET-E-SE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35550**	w.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	031121/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35556**		
Incorrect Authorization	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35559**		
N/A	20-Oct-21	5.1	Vulnerability in the Java SE product of Oracle Java SE (component: Deployment). The supported version that is affected is Java SE: 8u301. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35560**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Utility). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35561**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Keytool). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35564**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35565**		
N/A	20-Oct-21	6.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets,	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-35567**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35578**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35586**		
N/A	20-Oct-21	2.6	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u311, 8u301; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35588**		
N/A	20-Oct-21	4.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35603**		
e-series_santricity_web_services					
Incorrect Authorization	20-Oct-21	7.1	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35550**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35556**		
Incorrect Authorization	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35559**		
N/A	20-Oct-21	5.1	Vulnerability in the Java SE product of Oracle Java SE (component: Deployment). The supported version that is affected is Java SE: 8u301. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE.	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35560**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Utility). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35561**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Keytool). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0.	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-	A-NET-E-SE-031121/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35564**	20211022-0004/	
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311,	https://www.oracle.com/security-alerts/cpuoct2021.html, https://secu	A-NET-E-SE-031121/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35565**	rity.netapp.com/advisory/ntap-20211022-0004/	
N/A	20-Oct-21	6.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-35567**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35578**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/303
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpuoct2021.html, https://secu	A-NET-E-SE-031121/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35586**	rity.netapp.com/advisory/ntap-20211022-0004/	
N/A	20-Oct-21	2.6	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle	https://www.oracle.com/security-	A-NET-E-SE-031121/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u311, 8u301; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector:	alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35588**		
N/A	20-Oct-21	4.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Confidentiality impacts).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-E-SE-031121/306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35603**		
hci_management_node					
N/A	20-Oct-21	6.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-HCI_-031121/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-35567**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-HCI_-031121/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35586**		
N/A	20-Oct-21	2.6	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u311, 8u301; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-HCI_-031121/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35588**		
N/A	20-Oct-21	4.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE,	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-HCI_-031121/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35603**		
oncommand_insight					
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35537**		
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35546**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/312
Incorrect Authorization	20-Oct-21	7.1	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311,	https://www.oracle.com/security-alerts/cpuoct2021.html, https://secu	A-NET-ONCO-031121/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35550**	rity.netapp.com/advisory/ntap-20211022-0004/	
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing).	https://www.oracle.com/security-alerts/cpuoc	A-NET-ONCO-031121/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35556**	t2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	
Incorrect	20-Oct-21	5	Vulnerability in the Java SE,	https://ww	A-NET-ONCO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35559**	w.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	031121/315

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	5.1	Vulnerability in the Java SE product of Oracle Java SE (component: Deployment). The supported version that is affected is Java SE: 8u301. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35560**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-ONCO-031121/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Utility). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-ONCO-031121/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35561		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Keytool). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-ONCO-031121/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35564**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35565**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-ONCO-031121/319
N/A	20-Oct-21	6.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise	https://www.oracle.com	A-NET-ONCO-031121/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified	/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-35567**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35575**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/321
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory	A-NET-ONCO-031121/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via MySQL Protcol to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35577**	/ntap-20211022-0003/	
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-ONCO-031121/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35578**		
N/A	20-Oct-21	5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Windows). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35583**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/324
N/A	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: ndbcluster/plugin DDL). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory	A-NET-ONCO-031121/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35584**	/ntap-20211022-0003/	
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-ONCO-031121/326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35586**		
N/A	20-Oct-21	2.6	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u311, 8u301; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-ONCO-031121/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35588**		
Improper Input Validation	20-Oct-21	6.5	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35590**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35591**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/329
Improper Input Validation	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported	https://www.oracle.com/security-alerts/cpuoc	A-NET-ONCO-031121/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35592**	t2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	
Out-of-bounds Write	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35593**		
Improper Input Validation	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35594**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Error Handling). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35596**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/333
Improper Input Validation	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35598**		
N/A	20-Oct-21	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35602		
N/A	20-Oct-21	4.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-ONCO-031121/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35603**		
N/A	20-Oct-21	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.35 and prior and 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35604**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/337
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35607**		
N/A	20-Oct-21	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35608**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/339
N/A	20-Oct-21	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily	https://www.oracle.com/security-alerts/cpuoct2021.html, https://secu	A-NET-ONCO-031121/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35610**	rity.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35612**		
N/A	20-Oct-21	4.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35613**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/342
N/A	20-Oct-21	1.4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-	A-NET-ONCO-031121/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 1.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35618**	0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster.	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35621**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35622**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/345
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-	A-NET-ONCO-031121/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35623**	0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.35 and prior and 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2021-35624**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/347
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges).	https://www.oracle.com/security-alerts/cpuoc	A-NET-ONCO-031121/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35625**	t2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35626		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35627**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/350
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35628**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35629**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/352
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-	A-NET-ONCO-031121/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2021-35630**	0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35631**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/354
N/A	20-Oct-21	2.1	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Data Dictionary). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpuoct2021.html,	A-NET-ONCO-031121/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35632**	https://security.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35633		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35634**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/357
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35635**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35636**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/359
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-	A-NET-ONCO-031121/360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35637**	0003/	
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35638**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/361
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are	https://www.oracle.com/security-alerts/cpuoct2021.html,	A-NET-ONCO-031121/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35639**	https://security.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35640**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/363
N/A	20-Oct-21	4	Vulnerability in the MySQL	https://ww	A-NET-ONCO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35641**	w.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	031121/364
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35642**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35643**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/366
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35644**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35645**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/368
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily	https://www.oracle.com/security-alerts/cpuoct2021.html, https://secu	A-NET-ONCO-031121/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35646**	rity.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35647**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35648**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/371
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2478**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2479**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/373
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-ONCO-031121/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2481**		
santricity_unified_manager					
Incorrect Authorization	20-Oct-21	7.1	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SANT-031121/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35550**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SANT-031121/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35556**		
Incorrect Authorization	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SANT-031121/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35559**		
N/A	20-Oct-21	5.1	Vulnerability in the Java SE product of Oracle Java SE (component: Deployment). The supported version that is affected is Java SE: 8u301. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SANT-031121/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35560**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Utility). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SANT-031121/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35561**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Keytool). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SANT-031121/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35564**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SANT-031121/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35565**		
N/A	20-Oct-21	6.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Oracle GraalVM Enterprise Edition, attacks may significantly impact	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SANT-031121/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-35567**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SANT-031121/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35578**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SANT-031121/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35586**		
N/A	20-Oct-21	2.6	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u311, 8u301; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SANT-031121/385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35588**		
N/A	20-Oct-21	4.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.c	A-NET-SANT-031121/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35603**	om/advisory/ntap-20211022-0004/	
snapcenter					
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25	https://www.oracle.com/security-alerts/cpuoct2021.html,	A-NET-SNAP-031121/387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35537**	https://security.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35546**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35575**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/389
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via MySQL Protcol to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35577**		
N/A	20-Oct-21	5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Windows). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35583**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/391
N/A	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: ndbcluster/plugin DDL). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35584**		
Improper Input Validation	20-Oct-21	6.5	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35590		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35591**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/394
Improper Input Validation	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35592**		
Out-of-bounds Write	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35593		
Improper Input Validation	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35594**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/397
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Error Handling). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-	A-NET-SNAP-031121/398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35596**	0003/	
Improper Input Validation	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35598**		
N/A	20-Oct-21	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35602**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/400
N/A	20-Oct-21	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.35 and prior and 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35604**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35607**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/402
N/A	20-Oct-21	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://www.oracle.com/security-	A-NET-SNAP-031121/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Group Replication Plugin). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35608**	alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35610**		
N/A	20-Oct-21	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35612**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/405
N/A	20-Oct-21	4.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.26 and prior. Difficult to	https://www.oracle.com/security-alerts/cpuoct2021.html, https://secu	A-NET-SNAP-031121/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35613**	rity.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	1.4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 1.8 (Availability impacts).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35618**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35621**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/408
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.26 and prior. Easily exploitable	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.c	A-NET-SNAP-031121/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35622**	om/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35623**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/410
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle	https://www.oracle.com	A-NET-SNAP-031121/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.35 and prior and 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2021-35624**	/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35625**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35626**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/413
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35627**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35628**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/415
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.c	A-NET-SNAP-031121/416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35629**	om/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2021-35630**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/417
N/A	20-Oct-21	4	Vulnerability in the MySQL	https://ww	A-NET-SNAP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35631**	w.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	031121/418
N/A	20-Oct-21	2.1	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Data Dictionary). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35632**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35633**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/420
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35634**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35635**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/422
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.c	A-NET-SNAP-031121/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35636**	om/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35637**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/424
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle	https://www.oracle.com	A-NET-SNAP-031121/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35638**	/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35639**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35640**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/427
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35641**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35642**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/429
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-	A-NET-SNAP-031121/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35643**	20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35644**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/431
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://www.oracle.com/security-	A-NET-SNAP-031121/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35645**	alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35646**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35647**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/434
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35648**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2478**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/436
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-	A-NET-SNAP-031121/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2479**	0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2481**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-NET-SNAP-031121/438
solidfire					
N/A	20-Oct-21	6.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle	https://www.oracle.com/security-	A-NET-SOLI-031121/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a	alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web service which supplies data to the APIs. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-35567**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SOLI-031121/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35586**		
N/A	20-Oct-21	2.6	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u311, 8u301; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SOLI-031121/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35588**		
N/A	20-Oct-21	4.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-NET-SOLI-031121/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35603**		
netty					
netty					
Uncontrolled Resource Consumption	19-Oct-21	5	The Bzip2 decompression decoder function doesn't allow setting size restrictions on the decompressed output data (which affects the allocation size used during decompression). All users of Bzip2Decoder are affected. The malicious input can trigger an OOME and so a DoS attack **CVE ID : CVE-2021-37136**	N/A	A-NET-NETT-031121/443
Uncontrolled Resource Consumption	19-Oct-21	5	The Snappy frame decoder function doesn't restrict the chunk length which may lead to excessive memory usage. Beside this it also may buffer	N/A	A-NET-NETT-031121/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reserved skippable chunks until the whole chunk was received which may lead to excessive memory usage as well. This vulnerability can be triggered by supplying malicious input that decompresses to a very big size (via a network stream or a file) or by sending a huge skippable chunk. **CVE ID : CVE-2021-37137**		
Nextcloud					
contacts					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-21	3.5	Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud Contacts application prior to version 4.0.3 was vulnerable to a stored Cross-Site Scripting (XSS) vulnerability. For exploitation, a user would need to right-click on a malicious file and open the file in a new tab. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. It is recommended that the Nextcloud Contacts application is upgraded to 4.0.3. As a workaround, one may use a browser that has support for Content-Security-Policy. **CVE ID : CVE-2021-39221**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-j6cx-mxqf-f9vc	A-NEX-CONT-031121/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
deck					
Incorrect Authorization	25-Oct-21	5.5	Nextcloud is an open-source, self-hosted productivity platform. A missing permission check in Nextcloud Deck before 1.2.9, 1.4.5 and 1.5.3 allows another authenticated users to access Deck cards of another user. It is recommended that the Nextcloud Deck App is upgraded to 1.2.9, 1.4.5 or 1.5.3. There are no known workarounds aside from upgrading. **CVE ID : CVE-2021-39225**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-2x96-38qg-3m72, https://github.com/nextcloud/deck/pull/3316	A-NEX-DECK-031121/446
mail					
Exposure of Sensitive Information to an Unauthorized Actor	25-Oct-21	3.5	Nextcloud is an open-source, self-hosted productivity platform The Nextcloud Mail application prior to versions 1.10.4 and 1.11.0 does by default not render images in emails to not leak the read state or user IP. The privacy filter failed to filter images with a relative protocol. It is recommended that the Nextcloud Mail application is upgraded to 1.10.4 or 1.11.0. There are no known workarounds aside from upgrading. **CVE ID : CVE-2021-39220**	https://github.com/nextcloud/mail/pull/5470, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-6q9v-wm8r-rcv5	A-NEX-MAIL-031121/447
nextcloud_server					
Improper Control of Interaction	25-Oct-21	5.5	Nextcloud is an open-source, self-hosted productivity platform. Prior to versions	https://github.com/nextcloud/security	A-NEX-NEXT-031121/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Frequency			20.0.13, 21.0.5, and 22.2.0, Nextcloud Server did not implement a database backend for rate-limiting purposes. Any component of Nextcloud using rate-limits (as as `AnonRateThrottle` or `UserRateThrottle`) was thus not rate limited on instances not having a memory cache backend configured. In the case of a default installation, this would notably include the rate-limits on the two factor codes. It is recommended that the Nextcloud Server be upgraded to 20.0.13, 21.0.5, or 22.2.0. As a workaround, enable a memory cache backend in `config.php`. **CVE ID : CVE-2021-41177**	-advisories/security/advisories/GHSA-fj39-4qx4-m3f2, https://github.com/nextcloud/server/pull/28728	
officeonline					
N/A	25-Oct-21	5	Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud OfficeOnline application prior to version 1.1.1 returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. (e.g. an attacker could see that the file `shared.txt` is located within `/files/$username/Myfolder/Mysubfolder/shared.txt`). It is recommended that the OfficeOnline application is upgraded to 1.1.1. As a	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-56wm-r6jm-3v9h, https://github.com/nextcloud/officeonline/pull/204	A-NEX-OFFI-031121/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			workaround, one may disable the OfficeOnline application in the app settings. **CVE ID : CVE-2021-39224**		
richdocuments					
N/A	25-Oct-21	5	Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud Richdocuments application prior to versions 3.8.6 and 4.2.3 returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. (e.g. an attacker could see that the file `shared.txt` is located within `/files/$username/Myfolder/Mysubfolder/shared.txt`). It is recommended that the Richdocuments application is upgraded to 3.8.6 or 4.2.3. As a workaround, disable the Richdocuments application in the app settings. **CVE ID : CVE-2021-39223**	https://github.com/nextcloud/richdocuments/pull/1760, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-rjcc-4cgj-6v93	A-NEX-RICH-031121/450
server					
Unrestricted Upload of File with Dangerous Type	25-Oct-21	4	Nextcloud is an open-source, self-hosted productivity platform. Prior to versions 20.0.13, 21.0.5, and 22.2.0, a file traversal vulnerability makes an attacker able to download arbitrary SVG images from the host system, including user provided files. This could also be leveraged into a XSS/phishing attack,	https://github.com/nextcloud/server/pull/28726, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-	A-NEX-SERV-031121/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an attacker could upload a malicious SVG file that mimics the Nextcloud login form and send a specially crafted link to victims. The XSS risk here is mitigated due to the fact that Nextcloud employs a strict Content-Security-Policy disallowing execution of arbitrary JavaScript. It is recommended that the Nextcloud Server be upgraded to 20.0.13, 21.0.5 or 22.2.0. There are no known workarounds aside from upgrading. **CVE ID : CVE-2021-41178**	jp9c-vpr3-m5rf	
Missing Critical Step in Authentication	25-Oct-21	4	Nextcloud is an open-source, self-hosted productivity platform. Prior to Nextcloud Server versions 20.0.13, 21.0.5, and 22.2.0, the Two-Factor Authentication wasn't enforced for pages marked as public. Any page marked as `@PublicPage` could thus be accessed with a valid user session that isn't authenticated. This particularly affects the Nextcloud Talk application, as this could be leveraged to gain access to any private chat channel without going through the Two-Factor flow. It is recommended that the Nextcloud Server be upgraded to 20.0.13, 21.0.5 or 22.2.0. There are no	https://github.com/nextcloud/server/pull/28725, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-7hvh-rc6f-px23	A-NEX-SERV-031121/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			known workarounds aside from upgrading. **CVE ID : CVE-2021-41179**		
Ninjaforms					
contact_form					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-21	3.5	The Ninja Forms Contact Form WordPress plugin before 3.5.8.2 does not sanitise and escape the custom class name of the form field created, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24381**	N/A	A-NIN-CONT-031121/453
nothings					
stb_image.h					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-Oct-21	4.3	An issue was discovered in stb stb_image.h 1.33 through 2.27. The HDR loader parsed truncated end-of-file RLE scanlines as an infinite sequence of zero-length runs. An attacker could potentially have caused denial of service in applications using stb_image by submitting crafted HDR files. **CVE ID : CVE-2021-42715**	N/A	A-NOT-STB_-031121/454
Buffer Copy without Checking Size of Input ('Classic Buffer	21-Oct-21	6.4	An issue was discovered in stb stb_image.h 2.27. The PNM loader incorrectly interpreted 16-bit PGM files as 8-bit when converting to RGBA, leading to a buffer	N/A	A-NOT-STB_-031121/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			overflow when later reinterpreting the result as a 16-bit buffer. An attacker could potentially have crashed a service using stb_image, or read up to 1024 bytes of non-consecutive heap data without control over the read location. **CVE ID : CVE-2021-42716**		
Nvidia					
gpu_display_driver					
NULL Pointer Dereference	27-Oct-21	2.1	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for private IOCTLs, where an attacker with local unprivileged system access may cause a NULL pointer dereference, which may lead to denial of service in a component beyond the vulnerable component. **CVE ID : CVE-2021-1115**	https://nvidia.custhelp.com/app/answers/detail/a_id/5230	A-NVI-GPU_-031121/456
NULL Pointer Dereference	27-Oct-21	2.1	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a NULL pointer dereference in the kernel, created within user mode code, may lead to a denial of service in the form of a system crash. **CVE ID : CVE-2021-1116**	https://nvidia.custhelp.com/app/answers/detail/a_id/5230	A-NVI-GPU_-031121/457
nxp					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mcuxpresso_software_development_kit					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-Oct-21	4.6	NXP MCUXpresso SDK v2.7.0 was discovered to contain a buffer overflow in the function USB_HostProcessCallback(). **CVE ID : CVE-2021-38258**	N/A	A-NXP-MCUX-031121/458
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-Oct-21	4.6	NXP MCUXpresso SDK v2.7.0 was discovered to contain a buffer overflow in the function USB_HostParseDeviceConfigurationDescriptor(). **CVE ID : CVE-2021-38260**	N/A	A-NXP-MCUX-031121/459
Omron					
cx-supervisor					
Out-of-bounds Read	19-Oct-21	6	Out-of-bounds read vulnerability in CX-Supervisor v4.0.0.13 and v4.0.0.16 allows an attacker with administrative privileges to cause information disclosure and/or arbitrary code execution by opening a specially crafted SCS project files. **CVE ID : CVE-2021-20836**	https://www.myomron.com/index.php?action=kb&article=1692	A-OMR-CX-S-031121/460
Onedesigns					
one_user_avatar					
Improper Neutralization of Input During Web Page Generation ('Cross-site	18-Oct-21	3.5	The One User Avatar WordPress plugin before 2.3.7 does not escape the link and target attributes of its shortcode, allowing users with a role as low as Contributor to perform	N/A	A-ONE-ONE_-031121/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Stored Cross-Site Scripting attacks **CVE ID : CVE-2021-24672**		
Cross-Site Request Forgery (CSRF)	18-Oct-21	4.3	The One User Avatar WordPress plugin before 2.3.7 does not check for CSRF when updating the Avatar in page where the [avatar_upload] shortcode is embed. As a result, attackers could make logged in user change their avatar via a CSRF attack **CVE ID : CVE-2021-24675**	N/A	A-ONE-ONE_-031121/462
onepeloton					
peloton					
Cleartext Storage of Sensitive Information	25-Oct-21	5	Exposure of senstive information to an unauthorised actor in the "com.onepeloton.erlich" mobile application up to and including version 1.7.22 allows a remote attacker to access developer files stored in an AWS S3 bucket, by reading credentials stored in plain text within the mobile application. **CVE ID : CVE-2021-40527**	https://twitter.com/ROPsicle/status/1438216078103044107?s=20	A-ONE-PELO-031121/463
online_student_admission_system_project					
online_student_admission_system					
Improper Neutralization of Special Elements used in an SQL Command	26-Oct-21	7.5	Online Student Admission System 1.0 is affected by an unauthenticated SQL injection bypass vulnerability in /admin/login.php.	N/A	A-ONL-ONLI-031121/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2021-37371**		
Unrestricted Upload of File with Dangerous Type	26-Oct-21	6.5	Online Student Admission System 1.0 is affected by an insecure file upload vulnerability. A low privileged user can upload malicious PHP files by updating their profile image to gain remote code execution. **CVE ID : CVE-2021-37372**	N/A	A-ONL-ONLI-031121/465
openclinic_ga_project					
openclinic_ga					
Incorrect Permission Assignment for Critical Resource	26-Oct-21	9.3	OpenClinic GA 5.194.18 is affected by Insecure Permissions. By default the Authenticated Users group has the modify permission to openclinic folders/files. A low privilege account is able to rename mysqld.exe or tomcat8.exe files located in bin folders and replace with a malicious file that would connect back to an attacking computer giving system level privileges (nt authority\system) due to the service running as Local System. While a low privilege user is unable to restart the service through the application, a restart of the computer triggers the execution of the malicious file. The application also have unquoted service path issues.	N/A	A-OPE-OPEN-031121/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-37364		
Oracle					
applications_framework					
N/A	20-Oct-21	5	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Session Management). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Applications Framework. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-2477**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-APPL-031121/467
applications_manager					
N/A	20-Oct-21	8.5	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-APPL-031121/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-35566**		
N/A	20-Oct-21	6.8	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-APPL-031121/469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Applications Manager accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35569**		
N/A	20-Oct-21	5.8	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: View Reports). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data as well as unauthorized read access to a subset of Oracle Applications Manager accessible data. CVSS 3.1 Base Score 6.1	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-APPL-031121/470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2021-35580**		
N/A	20-Oct-21	4.3	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: View Reports). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2021-35581**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-APPL-031121/471
N/A	20-Oct-21	6	Vulnerability in the Oracle Applications Manager	https://www.oracle.com	A-ORA-APPL-031121/472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			product of Oracle E-Business Suite (component: View Reports). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data as well as unauthorized read access to a subset of Oracle Applications Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Applications Manager. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2021-35582**	/security-alerts/cpuoct2021.html	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
communications_interactive_session_recorder					
N/A	20-Oct-21	7.5	Vulnerability in the Oracle Communications Interactive Session Recorder product of Oracle Communications (component: Provision API). The supported version that is affected is 6.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Interactive Session Recorder. While the vulnerability is in Oracle Communications Interactive Session Recorder, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Interactive Session Recorder accessible data as well as unauthorized read access to a subset of Oracle Communications Interactive Session Recorder accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Communications Interactive Session Recorder. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-COMM-031121/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2021-2461**		
communications_session_border_controller					
N/A	20-Oct-21	6.8	Vulnerability in the Oracle Communications Session Border Controller product of Oracle Communications (component: Routing). Supported versions that are affected are 8.4 and 9.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Communications Session Border Controller. While the vulnerability is in Oracle Communications Session Border Controller, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications Session Border Controller accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-2414**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-COMM-031121/474
N/A	20-Oct-21	6.8	Vulnerability in the Oracle Communications Session Border Controller product of	https://www.oracle.com/security-	A-ORA-COMM-031121/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Communications (component: Routing). Supported versions that are affected are 8.4 and 9.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Communications Session Border Controller. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Communications Session Border Controller. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2416**	alerts/cpuoct2021.html	
content_manager					
N/A	20-Oct-21	5.5	Vulnerability in the Oracle Content Manager product of Oracle E-Business Suite (component: Content Item Manager). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Content Manager. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-CONT-031121/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			creation, deletion or modification access to critical data or all Oracle Content Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Content Manager accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-2483**		
database					
Incorrect Authorization	20-Oct-21	5.5	Vulnerability in the RDBMS Security component of Oracle Database Server. Supported versions that are affected are 12.2.0.1, 19c and 21c. Easily exploitable vulnerability allows high privileged attacker having DBA privilege with network access via Oracle Net to compromise RDBMS Security. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of RDBMS Security as well as unauthorized update, insert or delete access to some of RDBMS Security accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-DATA-031121/477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35551**		
N/A	20-Oct-21	4	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Table privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Core RDBMS. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35557**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-DATA-031121/478
N/A	20-Oct-21	4	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Table privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-DATA-031121/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (partial DOS) of Core RDBMS. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35558**		
database_server					
N/A	20-Oct-21	4	Vulnerability in the Oracle Database Enterprise Edition Unified Audit component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Local Logon privilege with network access via Oracle Net to compromise Oracle Database Enterprise Edition Unified Audit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database Enterprise Edition Unified Audit accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35576**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-DATA-031121/480
N/A	20-Oct-21	6.5	Vulnerability in the Oracle LogMiner component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-DATA-031121/481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA privilege with network access via Oracle Net to compromise Oracle LogMiner. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle LogMiner accessible data as well as unauthorized read access to a subset of Oracle LogMiner accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle LogMiner. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H). **CVE ID : CVE-2021-2332**		
deal_management					
N/A	20-Oct-21	5.5	Vulnerability in the Oracle Deal Management product of Oracle E-Business Suite (component: Miscellaneous). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Deal Management. Successful	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-DEAL-031121/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Deal Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Deal Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-35536**		
enterprise_manager_base_platform					
N/A	20-Oct-21	6.5	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Policy Framework). Supported versions that are affected are 13.4.0.0 and 13.5.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-ENTE-031121/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2137**		
essbase_administration_services					
N/A	20-Oct-21	7.5	Vulnerability in the Essbase Administration Services product of Oracle Essbase (component: EAS Console). The supported version that is affected is Prior to 11.1.2.4.046. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Essbase Administration Services. While the vulnerability is in Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Essbase Administration Services accessible data as well as unauthorized update, insert or delete access to some of Essbase Administration Services accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-35651**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-ESSB-031121/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	7.5	Vulnerability in the Essbase Administration Services product of Oracle Essbase (component: EAS Console). The supported version that is affected is Prior to 11.1.2.4.046. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Essbase Administration Services. While the vulnerability is in Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Essbase Administration Services. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2021-35652**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-ESSB-031121/485
N/A	20-Oct-21	6.8	Vulnerability in the Essbase Administration Services product of Oracle Essbase (component: EAS Console). The supported version that is affected is Prior to 11.1.2.4.046. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-ESSB-031121/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromise Essbase Administration Services. While the vulnerability is in Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Essbase Administration Services accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-35653**		
N/A	20-Oct-21	5	Vulnerability in the Essbase Administration Services product of Oracle Essbase (component: EAS Console). The supported version that is affected is Prior to 11.1.2.4.046. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Essbase Administration Services. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Essbase Administration Services.	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-ESSB-031121/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35654**		
N/A	20-Oct-21	5	Vulnerability in the Essbase Administration Services product of Oracle Essbase (component: EAS Console). The supported version that is affected is Prior to 11.1.2.4.046. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Essbase Administration Services. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Essbase Administration Services accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35655**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-ESSB-031121/488
graalvm					
Incorrect Authorization	20-Oct-21	7.1	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.c	A-ORA-GRAA-031121/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35550**	om/advisory/ntap-20211022-0004/	
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are	https://www.oracle.com/security-alerts/cpuoct2021.html,	A-ORA-GRAA-031121/490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35556**	https://security.netapp.com/advisory/ntap-20211022-0004/	
Incorrect Authorization	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise	https://www.oracle.com	A-ORA-GRAA-031121/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35559**	/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Utility). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-GRAA-031121/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35561		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Keytool). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-GRAA-031121/493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35564**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35565**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-GRAA-031121/494
N/A	20-Oct-21	6.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise	https://www.oracle.com	A-ORA-GRAA-031121/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified	/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-35567**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-GRAA-031121/496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35578**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-GRAA-031121/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35586**		
N/A	20-Oct-21	2.6	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u311, 8u301; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-GRAA-031121/498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35588**		
N/A	20-Oct-21	4.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-GRAA-031121/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35603**		
http_server					
N/A	20-Oct-21	7.1	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: OSSL Module). The supported version that is affected is 11.1.1.9.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle HTTP Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35666**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-HTTP-031121/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	4.3	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Web Listener). The supported version that is affected is 11.1.1.9.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle HTTP Server accessible data. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-2480**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-HTTP-031121/501
hyperion_financial_reporting					
N/A	20-Oct-21	5.8	Vulnerability in the Hyperion Financial Reporting product of Oracle Hyperion (component: Repository). The supported version that is affected is 11.2.6.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker and while the	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-HYPE-031121/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in Hyperion Financial Reporting, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2021-35665**		
incentive_compensation					
N/A	20-Oct-21	5.5	Vulnerability in the Oracle Incentive Compensation product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Incentive Compensation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-INCE-031121/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Incentive Compensation accessible data as well as unauthorized access to critical data or complete access to all Oracle Incentive Compensation accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-35585**		
java_virtual_machine					
N/A	20-Oct-21	4.6	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 19c and 21c. Difficult to exploit vulnerability allows low privileged attacker having Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35619**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-JAVA-031121/504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mobile_field_service					
N/A	20-Oct-21	8.5	Vulnerability in the Oracle Mobile Field Service product of Oracle E-Business Suite (component: Admin UI). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Mobile Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Mobile Field Service accessible data as well as unauthorized access to critical data or complete access to all Oracle Mobile Field Service accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-35570**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-MOBI-031121/505
mysql					
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.c	A-ORA-MYSQ-031121/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35537**	om/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35546**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/507
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle	https://www.oracle.com	A-ORA-MYSQ-031121/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35591**	/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Error Handling). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35596**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35597**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0005/	A-ORA-MYSQ-031121/510
N/A	20-Oct-21	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35610**		
N/A	20-Oct-21	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35612**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/512
N/A	20-Oct-21	1.4	Vulnerability in the MySQL	https://ww	A-ORA-MYSQ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 1.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35618**	w.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	031121/513
N/A	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35621**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35622**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/515
N/A	20-Oct-21	4	Vulnerability in the MySQL	https://ww	A-ORA-MYSQ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35623**	w.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	031121/516
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.35 and prior and 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2021-35624**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35625**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/518
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35626**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35627**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/520
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.c	A-ORA-MYSQ-031121/521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35628**	om/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35629**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/522
N/A	20-Oct-21	4	Vulnerability in the MySQL	https://ww	A-ORA-MYSQ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2021-35630**	w.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	031121/523
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts).	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35631**		
N/A	20-Oct-21	2.1	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Data Dictionary). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35632**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/525
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35633**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35634**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/527
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.c	A-ORA-MYSQ-031121/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35635**	om/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35636**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/529
N/A	20-Oct-21	6.8	Vulnerability in the MySQL	https://ww	A-ORA-MYSQ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35637**	w.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	031121/530
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35638**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35640**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/532
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35641**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35642**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/534
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-	A-ORA-MYSQ-031121/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35643**	20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35644**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/536
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://www.oracle.com/security-	A-ORA-MYSQ-031121/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35645**	alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35646**		
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35647**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/539
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35648**		
N/A	20-Oct-21	7.9	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Connectors accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. CVSS 3.1 Base Score 5.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:H). **CVE ID : CVE-2021-2471**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-MYSQ-031121/541
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions	https://www.oracle.com/security-alerts/cpuoc	A-ORA-MYSQ-031121/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2478**	t2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2479**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2481**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/544
mysql_cluster					
N/A	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: ndbcluster/plugin DDL). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DOS) of MySQL Cluster. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35584**		
Improper Input Validation	20-Oct-21	6.5	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35590**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/546
Improper Input Validation	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported	https://www.oracle.com/security-alerts/cpuoc	A-ORA-MYSQ-031121/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35592**	t2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	
Out-of-bounds Write	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35593**		
Improper Input Validation	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35594**		
Improper Input Validation	20-Oct-21	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35598**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/550
N/A	20-Oct-21	4.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows unauthenticated attacker	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory	A-ORA-MYSQ-031121/551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35613**	/ntap-20211022-0003/	
mysql_server					
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35575**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/552
N/A	20-Oct-21	4	Vulnerability in the MySQL	https://ww	A-ORA-MYSQ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via MySQL Protcol to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35577**	w.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	031121/553
N/A	20-Oct-21	5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Windows). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 7.5	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35583**		
N/A	20-Oct-21	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35602**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/555
N/A	20-Oct-21	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.35 and prior and 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-	A-ORA-MYSQ-031121/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-35604**	20211022-0003/	
N/A	20-Oct-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35607**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35608**	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/558
N/A	20-Oct-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0003/	A-ORA-MYSQ-031121/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35639**		
openjdk					
Incorrect Authorization	20-Oct-21	7.1	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-OPEN-031121/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35550**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-OPEN-031121/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35556**		
Incorrect Authorization	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-OPEN-031121/562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35559**		
N/A	20-Oct-21	5.1	Vulnerability in the Java SE product of Oracle Java SE (component: Deployment). The supported version that is affected is Java SE: 8u301. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-OPEN-031121/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35560**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Utility). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-OPEN-031121/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35561**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Keytool). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments,	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-OPEN-031121/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35564**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-OPEN-031121/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35565**		
N/A	20-Oct-21	6.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-OPEN-031121/567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-35567**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-OPEN-031121/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35578**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-OPEN-031121/569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35586**		
N/A	20-Oct-21	2.6	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u311, 8u301; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	A-ORA-OPEN-031121/570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35588**		
N/A	20-Oct-21	4.3	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-	A-ORA-OPEN-031121/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35603**	0004/	
operations_intelligence					
N/A	20-Oct-21	5.5	Vulnerability in the Oracle Operations Intelligence product of Oracle E-Business Suite (component: BIS Operations Intelligence). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-OPER-031121/572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Operations Intelligence. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Operations Intelligence accessible data as well as unauthorized access to critical data or complete access to all Oracle Operations Intelligence accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-2484**		
outside_in_technology					
N/A	20-Oct-21	5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-OUTS-031121/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35572**		
N/A	20-Oct-21	5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-OUTS-031121/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35573**		
N/A	20-Oct-21	5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-OUTS-031121/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35574**		
N/A	20-Oct-21	5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-OUTS-031121/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35656**		
N/A	20-Oct-21	5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note:	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-OUTS-031121/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35657**		
N/A	20-Oct-21	5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-OUTS-031121/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35658**		
N/A	20-Oct-21	5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-OUTS-031121/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35659**		
N/A	20-Oct-21	5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs).	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-OUTS-031121/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35660**		
N/A	20-Oct-21	5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-OUTS-031121/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35661**		
N/A	20-Oct-21	5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-OUTS-031121/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35662**		
payables					
N/A	20-Oct-21	8.5	Vulnerability in the Oracle Payables product of Oracle E-Business Suite (component: Invoice Approvals). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Payables. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payables accessible data as well as unauthorized access to critical data or complete access to all Oracle Payables accessible data. CVSS 3.1 Base Score 8.1	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-PAYA-031121/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-2482**		
peoplesoft_enterprise					
N/A	20-Oct-21	4.9	Vulnerability in the PeopleSoft Enterprise SCM product of Oracle PeopleSoft (component: Supplier Portal). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise SCM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-PEOP-031121/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2021-35541**		
peoplesoft_enterprise_cost_center_common_application_objects					
N/A	20-Oct-21	5.5	Vulnerability in the PeopleSoft Enterprise CC Common Application Objects product of Oracle PeopleSoft (component: Activity Guide Composer). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CC Common Application Objects. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise CC Common Application Objects accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise CC Common Application Objects accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-35543**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-PEOP-031121/585
peoplesoft_enterprise_cs_academic_advisement					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	5.5	Vulnerability in the PeopleSoft Enterprise CS Academic Advisement product of Oracle PeopleSoft (component: Advising Notes). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Academic Advisement. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise CS Academic Advisement accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise CS Academic Advisement accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2021-35571**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-PEOP-031121/586
peoplesoft_enterprise_cs_campus_community					
N/A	20-Oct-21	2.7	Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Notification Framework). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-PEOP-031121/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.0 and 9.2. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the PeopleSoft Enterprise CS Campus Community executes to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS Campus Community accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35606**		
peoplesoft_enterprise_cs_sa_integration_pack					
N/A	20-Oct-21	2.7	Vulnerability in the PeopleSoft Enterprise CS SA Integration Pack product of Oracle PeopleSoft (component: Students Administration). Supported versions that are affected are 9.0 and 9.2. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-PEOP-031121/588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PeopleSoft Enterprise CS SA Integration Pack executes to compromise PeopleSoft Enterprise CS SA Integration Pack. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS SA Integration Pack accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35601**		
peoplesoft_enterprise_cs_student_records					
Incorrect Authorization	20-Oct-21	6	Vulnerability in the PeopleSoft Enterprise CS Student Records product of Oracle PeopleSoft (component: Class Search). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Student Records. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise CS Student Records, attacks may significantly impact additional products.	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-PEOP-031121/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise CS Student Records accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise CS Student Records accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2021-35553**		
peoplesoft_enterprise_peopletools					
N/A	20-Oct-21	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Rich Text Editor). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products.	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-PEOP-031121/590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2021-35568**		
N/A	20-Oct-21	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Business Interlink). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-PEOP-031121/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2021-35595**		
N/A	20-Oct-21	4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: SQR). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-PEOP-031121/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35609**		
sales_offline					
Improper Input Validation	20-Oct-21	4	Vulnerability in the Oracle Sales Offline product of Oracle E-Business Suite (component: Offline Template). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sales Offline. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Sales Offline. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35611**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-SALE-031121/593
secure_global_desktop					
N/A	20-Oct-21	5.5	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Server). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle Secure Global	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-SECU-031121/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Desktop. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Secure Global Desktop accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Secure Global Desktop. CVSS 3.1 Base Score 5.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L). **CVE ID : CVE-2021-35649**		
N/A	20-Oct-21	4.9	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Client). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Secure Global Desktop accessible data and unauthorized ability to cause a partial denial of service	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-SECU-031121/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(partial DOS) of Oracle Secure Global Desktop. CVSS 3.1 Base Score 4.6 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2021-35650**		
shipping_execution					
N/A	20-Oct-21	8.5	Vulnerability in the Oracle Shipping Execution product of Oracle E-Business Suite (component: Workflow Events). Supported versions that are affected are 12.2.6-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Shipping Execution. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Shipping Execution accessible data as well as unauthorized access to critical data or complete access to all Oracle Shipping Execution accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-35563**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-SHIP-031121/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
trade_management					
N/A	20-Oct-21	5	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Quotes). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Trade Management accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-35554**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-TRAD-031121/597
N/A	20-Oct-21	5.5	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Quotes). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-TRAD-031121/598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			modification access to critical data or all Oracle Trade Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-2485**		
transportation_management					
N/A	20-Oct-21	5.5	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: UI Infrastructure). The supported version that is affected is 6.4.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data as well as unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.1	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-TRAN-031121/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2021-35616**		
N/A	20-Oct-21	5	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain (component: Authentication). The supported version that is affected is 6.4.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-2476**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-TRAN-031121/600
universal_work_queue					
N/A	20-Oct-21	8.5	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-UNIV-031121/601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Universal Work Queue accessible data as well as unauthorized access to critical data or complete access to all Oracle Universal Work Queue accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-35562**		
vm_virtualbox					
N/A	20-Oct-21	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox.	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-VM_V-031121/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: This vulnerability does not apply to Windows systems. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35538**		
N/A	20-Oct-21	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35540**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-VM_V-031121/603
N/A	20-Oct-21	4.9	Vulnerability in the Oracle VM VirtualBox product of	https://www.oracle.com	A-ORA-VM_V-031121/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35542**	/security-alerts/cpuoct2021.html	
N/A	20-Oct-21	5.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products.	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-VM_V-031121/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.7 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/ UI:N/S:C/C:L/I:N/A:H). **CVE ID : CVE-2021-35545**		
N/A	20-Oct-21	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-VM_V-031121/606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2475**		
weblogic_server					
Incorrect Authorization	20-Oct-21	5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Diagnostics). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35552**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-WEBL-031121/607
N/A	20-Oct-21	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Coherence Container). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-WEBL-031121/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35617**		
N/A	20-Oct-21	5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-35620**	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-WEBL-031121/609
web_analytics					
N/A	20-Oct-21	8.5	Vulnerability in the Oracle	https://ww	A-ORA-WEB_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Web Analytics product of Oracle E-Business Suite (component: Admin). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Web Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Web Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Web Analytics accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-2474**	w.oracle.com/security-alerts/cpuoct2021.html	031121/610
zero_downtime_db_migration_to_cloud					
N/A	20-Oct-21	4.6	Vulnerability in the Zero Downtime DB Migration to Cloud component of Oracle Database Server. The supported version that is affected is 21c. Easily exploitable vulnerability allows high privileged attacker having Local Logon privilege with logon to the infrastructure where Zero	https://www.oracle.com/security-alerts/cpuoct2021.html	A-ORA-ZERO-031121/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Downtime DB Migration to Cloud executes to compromise Zero Downtime DB Migration to Cloud. While the vulnerability is in Zero Downtime DB Migration to Cloud, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Zero Downtime DB Migration to Cloud. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2021-35599**		
origincode					
smart-grid-gallery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-21	3.5	The Video Gallery â€“ Vimeo and YouTube Gallery WordPress plugin through 1.1.4 does not escape the Title and Description of the videos in a gallery before outputting them in attributes, leading to Stored Cross-Site Scripting issues **CVE ID : CVE-2021-24515**	N/A	A-ORI-SMAR-031121/612
Otrs					
otrs					
Incorrect Permission Assignment for Critical	18-Oct-21	4	Agents are able to lock the ticket without the "Owner" permission. Once the ticket is locked, it could be moved	https://otrs.com/release-notes/otrs-security-	A-OTR-OTRS-031121/613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			to the queue where the agent has "rw" permissions and gain a full control. This issue affects: OTRS AG OTRS 8.0.x version: 8.0.16 and prior versions. **CVE ID : CVE-2021-36097**	advisory-2021-20/	
Owasp					
java_html_sanitizer					
Improper Input Validation	18-Oct-21	7.5	The OWASP Java HTML Sanitizer before 20211018.1 does not properly enforce policies associated with the SELECT, STYLE, and OPTION elements. **CVE ID : CVE-2021-42575**	N/A	A-OWA-JAVA-031121/614
Parallels					
parallels_desktop					
Allocation of Resources Without Limits or Throttling	25-Oct-21	7.2	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of user-supplied data, which can result in an uncontrolled memory allocation. An attacker can leverage this vulnerability to escalate privileges and	https://kb.parallels.com/125013	A-PAR-PARA-031121/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13544. **CVE ID : CVE-2021-34854**		
Use of Uninitialized Resource	25-Oct-21	2.1	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13592. **CVE ID : CVE-2021-34855**	https://kb.parallels.com/125013	A-PAR-PARA-031121/616
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-21	4.6	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the virtio-gpu virtual	https://kb.parallels.com/125013	A-PAR-PARA-031121/617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13581. **CVE ID : CVE-2021-34856**		
Out-of-bounds Write	25-Oct-21	4.6	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13601. **CVE ID : CVE-2021-34857**	https://kb.parallels.com/125013	A-PAR-PARA-031121/618
Improper Access Control	25-Oct-21	4.6	This vulnerability allows local attackers to escalate privileges on affected	N/A	A-PAR-PARA-031121/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the WinAppHelper component. The issue results from the lack of proper access control. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13543. **CVE ID : CVE-2021-34864**		
pdf_viewer_block_for_gutenberg_project					
pdf_viewer_block_for_gutenberg					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	The Gutenberg PDF Viewer Block WordPress plugin before 1.0.1 does not sanitise and escape its block, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks. **CVE ID : CVE-2021-24760**	N/A	A-PDF-PDF_-031121/620
permalink_manager_lite_project					
permalink_manager_lite					
Improper Neutralization of Special Elements used in an SQL	25-Oct-21	6.5	The Permalink Manager Lite WordPress plugin before 2.2.13.1 does not validate and escape the orderby parameter before using it in a SQL statement in the	N/A	A-PER-PERM-031121/621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			Permalink Manager page, leading to a SQL Injection **CVE ID : CVE-2021-24769**		
PHP					
php					
Out-of-bounds Write	25-Oct-21	7.2	In PHP versions 7.3.x up to and including 7.3.31, 7.4.x below 7.4.25 and 8.0.x below 8.0.12, when running PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower-privileged users, it is possible for the child processes to access memory shared with the main process and write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and writes, which can be used to escalate privileges from local unprivileged user to the root user. **CVE ID : CVE-2021-21703**	https://bugs.php.net/bug.php?id=81026	A-PHP-PHP-031121/622
pi-hole					
web_interface					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-21	3.5	Pi-hole's Web interface (based on AdminLTE) provides a central location to manage one's Pi-hole and review the statistics generated by FTLDNS. Prior to version 5.8, cross-site scripting is possible when adding a client via the	https://github.com/pi-hole/AdminLTE/security/advisories/GHSA-mhr8-7rvg-8r43, https://github.com/pi-	A-PI--WEB_-031121/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			groups-clients management page. This issue was patched in version 5.8. **CVE ID : CVE-2021-41175**	hole/AdminLTE/commit/01191c7a1b8d5032991ed9d88e0db8d3dbec744d	
planso					
planso_forms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	The PlanSo Forms WordPress plugin through 2.6.3 does not escape the title of its Form before outputting it in attributes, allowing high privilege users such as admin to set XSS payload in it, even when the unfiltered_html is disallowed, leading to an Authenticated Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24516**	N/A	A-PLA-PLAN-031121/624
Pocoo					
babel					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Oct-21	7.2	Babel.Locale in Babel before 2.9.1 allows attackers to load arbitrary locale .dat files (containing serialized Python objects) via directory traversal, leading to code execution. **CVE ID : CVE-2021-42771**	https://github.com/python-babel/babel/pull/782	A-POC-BABE-031121/625
portainer					
portainer					
Improper Neutralization of Input During Web	18-Oct-21	4.3	Cross Site Scripting (XSS vulnerability exists in Portainer before 2.9.1 via the node input box in	https://github.com/portainer/portainer/pull/5766	A-POR-PORT-031121/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			Custom Templates. **CVE ID : CVE-2021-42650**		
presstigers					
simple_job_board					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	3.5	The Simple Job Board WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping on the $job_board_privacy_policy_label variable echo'd out via the ~/admin/settings/class-simple-job-board-settings-privacy.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 2.9.4. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. **CVE ID : CVE-2021-39328**	https://plugins.trac.wordpress.org/changeset/2617364/simple-job-board/trunk/admin/settings/class-simple-job-board-settings-privacy.php	A-PRE-SIMP-031121/627
proof-of-stake_ethereum_project					
proof-of-stake_ethereum					
N/A	20-Oct-21	6.4	The Proof-of-Stake (PoS) Ethereum consensus protocol through 2021-10-19 allows an adversary to cause a denial of service (delayed consensus decisions), and also increase the profits of individual validators, via short-range reorganizations of the	N/A	A-PRO-PROO-031121/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			underlying consensus chain. **CVE ID : CVE-2021-42764**		
N/A	20-Oct-21	5	The Proof-of-Stake (PoS) Ethereum consensus protocol through 2021-10-19 allows an adversary to leverage network delay to cause a denial of service (indefinite stalling of consensus decisions). **CVE ID : CVE-2021-42765**	N/A	A-PRO-PROO-031121/629
N/A	20-Oct-21	6.4	The Proof-of-Stake (PoS) Ethereum consensus protocol through 2021-10-19 allows an adversary to cause a denial of service (long-range consensus chain reorganizations), even when this adversary has little stake and cannot influence network message propagation. This can cause a protocol stall, or an increase in the profits of individual validators. **CVE ID : CVE-2021-42766**	N/A	A-PRO-PROO-031121/630
pterodactyl					
panel					
Cross-Site Request Forgery (CSRF)	25-Oct-21	4.3	Pterodactyl is an open-source game server management panel built with PHP 7, React, and Go. In affected versions of Pterodactyl a malicious user can trigger a user logout if a signed in user visits a malicious website that makes a request to the	https://github.com/pterodactyl/panel/security/advisories/GHSA-m49f-hcxp-6hm6, https://github.com/pterodactyl/panel	A-PTE-PANE-031121/631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Panel's sign-out endpoint. This requires a targeted attack against a specific Panel instance, and serves only to sign a user out. **No user details are leaked, nor is any user data affected, this is simply an annoyance at worst.** This is fixed in version 1.6.3. **CVE ID : CVE-2021-41176**	/commit/45999ba4ee1b2dcb12b4a2fa2cedfb6b5d66fac2	
Python					
pybluemonday					
Improper Input Validation	18-Oct-21	7.5	The bluemonday sanitizer before 1.0.16 for Go, and before 0.0.8 for Python (in pybluemonday), does not properly enforce policies associated with the SELECT, STYLE, and OPTION elements. **CVE ID : CVE-2021-42576**	N/A	A-PYT-PYBL-031121/632
qutebrowser					
qutebrowser					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	21-Oct-21	6.8	qutebrowser is an open source keyboard-focused browser with a minimal GUI. Starting with qutebrowser v1.7.0, the Windows installer for qutebrowser registers a `qutebrowserurl:` URL handler. With certain applications, opening a specially crafted `qutebrowserurl:...` URL can lead to execution of qutebrowser commands, which in turn allows	https://github.com/qutebrowser/qutebrowser/security/advisories/GHSA-vw27-fwjf-5qxm, https://github.com/qutebrowser/qutebrowser/commit/8f46ba3f6dc7b183	A-QUT-QUTE-031121/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution via commands such as `:spawn` or `:debug-pyeval`. Only Windows installs where qutebrowser is registered as URL handler are affected. The issue has been fixed in qutebrowser v2.4.0. The fix also adds additional hardening for potential similar issues on Linux (by adding the new --untrusted-args flag to the .desktop file), though no such vulnerabilities are known. **CVE ID : CVE-2021-41146**	75f7aa63c48a1fe461190430	
rasa					
rasa					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Oct-21	5.8	Rasa is an open source machine learning framework to automate text-and voice-based conversations. In affected versions a vulnerability exists in the functionality that loads a trained model `tar.gz` file which allows a malicious actor to craft a `model.tar.gz` file which can overwrite or replace bot files in the bot directory. The vulnerability is fixed in Rasa 2.8.10. For users unable to update ensure that users do not upload untrusted model files, and restrict CLI or API endpoint access where a malicious actor could target a deployed Rasa instance.	https://github.com/RasaHQ/rasa/security/advisories/GHSA-4365-fhm5-qcrx, https://github.com/RasaHQ/rasa/commit/1b6b502f52d73b4f8cd1959ce724b8ad0eb33989	A-RAS-RASA-031121/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-41127		
rasa_x					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Oct-21	4.3	Rasa X before 0.42.4 allows Directory Traversal during archive extraction. In the functionality that allows a user to load a trained model archive, an attacker has arbitrary write capability within specific directories via a crafted archive file. **CVE ID : CVE-2021-42556**	https://github.com/RasaHQ/rasa-x-security-advisories/security/advisories/GHSA-vp2h-j6px-56rc	A-RAS-RASA-031121/635
reddit					
snudown					
Use of a Broken or Risky Cryptographic Algorithm	21-Oct-21	4	Snudown is a reddit-specific fork of the Sundown Markdown parser used by GitHub, with Python integration added. In affected versions snudown was found to be vulnerable to denial of service attacks to its reference table implementation. References written in markdown ` [reference_name]: https://www.example.com` are inserted into a hash table which was found to have a weak hash function, meaning that an attacker can reliably generate a large number of collisions for it. This makes the hash table vulnerable to a hash-collision DoS attack, a type of algorithmic complexity attack. Further the hash table allowed for duplicate entries resulting in	https://github.com/reddit/snudown/security/advisories/GHSA-6gvv-9q92-w5f6, https://github.com/reddit/snudown/commit/1ac2c130b210539ee1e5d67a7bac93f9d8007c0e	A-RED-SNUD-031121/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			long retrieval times. Proofs of concept and further discussion of the hash collision issue are discussed on the snudown GHSA(https://github.com/reddit/snudown/security/advisories/GHSA-6gvv-9q92-w5f6). Users are advised to update to version 1.7.0. **CVE ID : CVE-2021-41168**		
Redhat					
openshift					
Cleartext Storage of Sensitive Information	19-Oct-21	4	IBM Security Risk Manager on CP4S 1.7.0.0 stores user credentials in plain clear text which can be read by a an authenticatedl privileged user. IBM X-Force ID: 209940. **CVE ID : CVE-2021-38911**	https://exchange.xforce.ibmcloud.com/vulnerabilities/209940, https://www.ibm.com/support/pages/node/6505281	A-RED-OPEN-031121/637
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	IBM Security Risk Manager on CP4S 1.7.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 207828. **CVE ID : CVE-2021-29912**	https://exchange.xforce.ibmcloud.com/vulnerabilities/207828, https://www.ibm.com/support/pages/node/6505283	A-RED-OPEN-031121/638
revisorlab					
video_management_system					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-21	5	Revisor Video Management System (VMS) before 2.0.0 has a directory traversal vulnerability. Successful exploitation could allow an attacker to traverse the file system to access files or directories that are outside of restricted directory on the remote server. This could lead to the disclosure of sensitive data on the vulnerable server. **CVE ID : CVE-2021-42261**	https://revisorlab.com/	A-REV-VIDE-031121/639
Rubyonrails					
rails					
URL Redirection to Untrusted Site ('Open Redirect')	18-Oct-21	5.8	A possible open redirect vulnerability in the Host Authorization middleware in Action Pack >= 6.0.0 that could allow attackers to redirect users to a malicious website. **CVE ID : CVE-2021-22942**	https://weblog.rubyonrails.org/2021/8/19/Rails-6-0-4-1-and-6-1-4-1-have-been-released/	A-RUB-RAIL-031121/640
salesagility					
suitecrm					
Unrestricted Upload of File with Dangerous Type	22-Oct-21	9	SuiteCRM before 7.11.19 allows remote code execution via the system settings Log File Name setting. In certain circumstances involving admin account takeover, logger_file_name can refer to an attacker-controlled PHP file under the web root, because only the all-lowercase PHP file	https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_19, https://suitecrm.com/time-to-upgrade-suitecrm-7-11-19-7-10-30-lts-	A-SAL-SUIT-031121/641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			extensions were blocked. NOTE: this issue exists because of an incomplete fix for CVE-2020-28328. **CVE ID : CVE-2021-42840**	released/	
sandhillsdev					
easy_digital_downloads					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	3.5	The Easy Digital Downloads WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the $start_date and $end_date parameters found in the ~/includes/admin/payments/class-payments-table.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.11.2. **CVE ID : CVE-2021-39354**	https://plugins.trac.wordpress.org/changeset/2616149/easy-digital-downloads/trunk/includes/admin/payments/class-payments-table.php	A-SAN-EASY-031121/642
sanskruti					
st-daily-tip					
Cross-Site Request Forgery (CSRF)	25-Oct-21	6.8	The St-Daily-Tip WordPress plugin through 4.7 does not have any CSRF check in place when saving its 'Default Text to Display if no tips' setting, and was also lacking sanitisation as well as escaping before outputting it the page. This could allow attacker to make logged in administrators set a malicious payload in it, leading to a Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24487**	N/A	A-SAN-ST-D-031121/643
scroll_banner_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
scroll_banner					
Cross-Site Request Forgery (CSRF)	18-Oct-21	4.3	The Scroll Baner WordPress plugin through 1.0 does not have CSRF check in place when saving its settings, nor perform any sanitisation, escaping or validation on them. This could allow attackers to make logged in admin change them and could lead to RCE (via a file upload) as well as XSS **CVE ID : CVE-2021-24642**	N/A	A-SCR-SCRO-031121/644
secondlinethemes					
podcast_subscribe_buttons					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	The Podcast Subscribe Buttons WordPress plugin before 1.4.2 allows users with any role capable of editing or adding posts to perform stored XSS. **CVE ID : CVE-2021-24743**	N/A	A-SEC-PODC-031121/645
shell-quote_project					
shell-quote					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	21-Oct-21	7.5	The shell-quote package before 1.7.3 for Node.js allows command injection. An attacker can inject unescaped shell metacharacters through a regex designed to support Windows drive letters. If the output of this package is passed to a real shell as a quoted argument to a command with exec(), an attacker can inject arbitrary	https://github.com/substack/node-shell-quote/commit/5799416ed454aa4ec9afafc895b4e31760ea1abe, https://www.npmjs.com/package/shell-quote,	A-SHE-SHEL-031121/646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands. This is because the Windows drive letter regex character class is {A-z] instead of the correct {A-Za-z]. Several shell metacharacters exist in the space between capital letter Z and lower case letter a, such as the backtick character. **CVE ID : CVE-2021-42740**	https://github.com/substack/node-shell-quote/blob/master/CHANGELOG.md#173	
Shopware					
shopware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-21	3.5	Shopware is open source e-commerce software. Versions prior to 5.7.6 contain a cross-site scripting vulnerability. This issue is patched in version 5.7.6. Two workarounds are available. Using the security plugin or adding a particular following config to the `.htaccess` file will protect against cross-site scripting in this case. There is also a config for those using nginx as a server. The plugin and the configs can be found on the GitHub Security Advisory page for this vulnerability. **CVE ID : CVE-2021-41188**	https://github.com/shopware/shopware/commit/37213e91d525c95df262712cba80d1497e395a58, https://github.com/shopware/shopware/security/advisories/GHSA-4p3x-8qw9-24w9, https://docs.shopware.com/en/shopware-5-en/sicherheitsupdates/security-update-10-2021	A-SHO-SHOP-031121/647
showdoc					
showdoc					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	22-Oct-21	7.5	ShowDoc 2.8.3 ihas a file upload vulnerability, where attackers can use the vulnerability to obtain server permissions. **CVE ID : CVE-2021-41745**	N/A	A-SHO-SHOW-031121/648
signalwire					
freeswitch					
Missing Initialization of Resource	18-Oct-21	5	An issue was discovered in function sofia_handle_sip_i_notify in sofia.c in SignalWire freeswitch before 1.10.6, may allow attackers to view sensitive information due to an uninitialized value. **CVE ID : CVE-2021-36513**	https://github.com/signalwire/freeswitch/releases/tag/v1.10.6, https://newreleases.io/project/github/signalwire/freeswitch/release/v1.10.6	A-SIG-FREE-031121/649
simple_payroll_system_with_dynamic_tax_bracket_project					
simple_payroll_system_with_dynamic_tax_bracket					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Oct-21	7.5	The Simple Payroll System with Dynamic Tax Bracket in PHP using SQLite Free Source Code (by: oretnom23) is vulnerable from remote SQL-Injection-Bypass-Authentication for the admin account. The parameter (username) from the login form is not protected correctly and there is no security and escaping from malicious payloads. **CVE ID : CVE-2021-42169**	N/A	A-SIM-SIMP-031121/650
Sixapart					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
movable_type					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Oct-21	7.5	Movable Type 7 r.5002 and earlier (Movable Type 7 Series), Movable Type 6.8.2 and earlier (Movable Type 6 Series), Movable Type Advanced 7 r.5002 and earlier (Movable Type Advanced 7 Series), Movable Type Advanced 6.8.2 and earlier (Movable Type Advanced 6 Series), Movable Type Premium 1.46 and earlier, and Movable Type Premium Advanced 1.46 and earlier allow remote attackers to execute arbitrary OS commands via unspecified vectors. Note that all versions of Movable Type 4.0 or later including unsupported (End-of-Life, EOL) versions are also affected by this vulnerability. **CVE ID : CVE-2021-20837**	https://movabletype.org/news/2021/10/mt-782-683-released.html	A-SIX-MOVA-031121/651
snipeitapp					
snipe-it					
Cross-Site Request Forgery (CSRF)	19-Oct-21	6.8	snipe-it is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-3858**	https://huntr.dev/bounties/a2fac2eb-100d-45b1-9ac7-71847c2f2b6b, https://github.com/snipe/snipe-it/commit/84c73aae5dca	A-SNI-SNIP-031121/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				fa9529ceeeda6e8cdda5a42129c3	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	4.3	snipe-it is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3863**	https://huntr.dev/bounties/1dbc8d79-1b53-44a3-a576-faec78f29ba0, https://github.com/snipe/snipe-it/commit/fc5efd857f61f7e45c61db567bb66612bcb53128	A-SNI-SNIP-031121/653
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	snipe-it is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3879**	https://github.com/snipe/snipe-it/commit/bda23bb1e66fd7ce42c75c69cf5eea4e80865c1c, https://huntr.dev/bounties/6dccc49e-3843-4a4a-b397-5c659e5f8bfe	A-SNI-SNIP-031121/654
Snort					
snort					
Missing Release of Memory after Effective	27-Oct-21	7.8	Multiple Cisco products are affected by a vulnerability in the way the Snort detection engine processes ICMP	https://tools.cisco.com/security/center/content/Cis	A-SNO-SNOR-031121/655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Lifetime			traffic that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper memory resource management while the Snort detection engine is processing ICMP packets. An attacker could exploit this vulnerability by sending a series of ICMP packets through an affected device. A successful exploit could allow the attacker to exhaust resources on the affected device, causing the device to reload. **CVE ID : CVE-2021-40114**	coSecurityAdvisory/cisco-sa-snort-dos-s2R7W9UU	
N/A	27-Oct-21	7.1	Multiple Cisco products are affected by a vulnerability in Snort rules that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.The vulnerability is due to improper handling of the Block with Reset or Interactive Block with Reset actions if a rule is configured without proper constraints. An attacker could exploit this vulnerability by sending a crafted IP packet to the affected device. A successful exploit could allow the attacker to cause through traffic to be dropped. Note:	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-RywH7ezM	A-SNO-SNOR-031121/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Only products with Snort3 configured and either a rule with Block with Reset or Interactive Block with Reset actions configured are vulnerable. Products configured with Snort2 are not vulnerable. **CVE ID : CVE-2021-40116**		
sociable_project					
sociable					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	The Sociable WordPress plugin through 4.3.4.1 does not sanitise or escape some of its settings before outputting them in the admins dashboard, allowing high privilege users to perform Cross-Site Scripting attacks against other users even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24612**	N/A	A-SOC-SOCI-031121/657
Solarwinds					
access_rights_manager					
Deserialization of Untrusted Data	21-Oct-21	4.6	The HTTP interface was enabled for RabbitMQ Plugin in ARM 2020.2.6 and the ability to configure HTTPS was not available. **CVE ID : CVE-2021-35227**	https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35227, https://documentation.solarwinds.com/en/succes	A-SOL-ACCE-031121/658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				s_center/arm/content/release_notes/arm_2021-4_release_notes.htm	
database_performance_analyzer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	2.6	This vulnerability occurred due to missing input sanitization for one of the output fields that is extracted from headers on specific section of page causing a reflective cross site scripting attack. An attacker would need to perform a Man in the Middle attack in order to change header for a remote victim. **CVE ID : CVE-2021-35228**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2021-35228, https://documentation.solarwinds.com/en/success_center/dpa/content/release_notes/dpa_2021-3-7438_release_notes.htm	A-SOL-DATA-031121/659
kiwi_cattools					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Oct-21	7.2	As a result of an unquoted service path vulnerability present in the Kiwi CatTools Installation Wizard, a local attacker could gain escalated privileges by inserting an executable into the path of the affected service or uninstall entry. **CVE ID : CVE-2021-35230**	https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35230	A-SOL-KIWI-031121/660
kiwi_syslog_server					
Unquoted Search Path	25-Oct-21	4.6	As a result of an unquoted service path vulnerability	https://documentation.so	A-SOL-KIWI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
or Element			present in the Kiwi Syslog Server Installation Wizard, a local attacker could gain escalated privileges by inserting an executable into the path of the affected service or uninstall entry. Example vulnerable path: "Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Kiwi Syslog Server\Parameters\Application". **CVE ID : CVE-2021-35231**	larwinds.com/en/success_center/kss/content/release_notes/kss_9-8_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35231	031121/661
N/A	27-Oct-21	5	The HTTP TRACK & TRACE methods were enabled in Kiwi Syslog Server 9.7.1 and earlier. These methods are intended for diagnostic purposes only. If enabled, the web server will respond to requests that use these methods by returning exact HTTP request that was received in the response to the client. This may lead to the disclosure of sensitive information such as internal authentication headers appended by reverse proxies. **CVE ID : CVE-2021-35233**	https://documentation.solarwinds.com/en/success_center/kss/content/release_notes/kss_9-8_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2021-35233	A-SOL-KIWI-031121/662
N/A	27-Oct-21	5	The ASP.NET debug feature is enabled by default in Kiwi Syslog Server 9.7.2 and previous versions. ASP.NET allows remote debugging of web applications, if	https://documentation.solarwinds.com/en/success_center/kss/content/rel	A-SOL-KIWI-031121/663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configured to do so. Debug mode causes ASP.NET to compile applications with extra information. The information enables a debugger to closely monitor and control the execution of an application. If an attacker could successfully start a remote debugging session, this is likely to disclose sensitive information about the web application and supporting infrastructure that may be valuable in targeting SWI with malicious intent. **CVE ID : CVE-2021-35235**	ease_notes/kss_9-8_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2021-35235	
Missing Encryption of Sensitive Data	27-Oct-21	5	The Secure flag is not set in the SSL Cookie of Kiwi Syslog Server 9.7.2 and previous versions. The Secure attribute tells the browser to only send the cookie if the request is being sent over a secure channel such as HTTPS. This will help protect the cookie from being passed over unencrypted requests. If the application can be accessed over both HTTP, there is a potential for the cookie can be sent in clear text. **CVE ID : CVE-2021-35236**	https://documentation.solarwinds.com/en/success_center/kss/content/release_notes/kss_9-8_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35236	A-SOL-KIWI-031121/664
network_performance_monitor					
Improper Privilege	21-Oct-21	5.5	Each authenticated Orion Platform user in a MSP (Managed Service Provider)	https://documentation.solarwinds.co	A-SOL-NETW-031121/665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			environment can view and browse all NetPath Services from all that MSP's customers. This can lead to any user having a limited insight into other customer's infrastructure and potential data cross-contamination. **CVE ID : CVE-2021-35225**	m/en/success_center/orionplatform/content/core-secure-configuration.htm, https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35225	
sourcecodester					
news247_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-21	4.3	Cross Site Scripting (XSS) vulnerability exists in Sourcecodester News247 CMS 1.0 via the search function in articles. **CVE ID : CVE-2021-41728**	N/A	A-SOU-NEWS-031121/666
Squid-cache					
squid					
Improper Certificate Validation	18-Oct-21	5	An issue was discovered in Squid 5.0.6 through 5.1.x before 5.2. When validating an origin server or peer certificate, Squid may incorrectly classify certain certificates as trusted. This problem allows a remote server to obtain security trust well improperly. This indication of trust may be passed along to clients,	http://www.squid-cache.org/Versions/v6/changesets/squid-6-43d6b5c81b88ec2256b430c69a872a1e4f324e4a.patch, https://githu	A-SQU-SQUI-031121/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowing access to unsafe or hijacked services. **CVE ID : CVE-2021-41611**	b.com/squid-cache/squid/security/advisories/GHSA-47m4-g3mv-9q5r	
Stanford					
corenlp					
Improper Restriction of XML External Entity Reference	19-Oct-21	5	corenlp is vulnerable to Improper Restriction of XML External Entity Reference **CVE ID : CVE-2021-3869**	https://github.com/stanfordnlp/corenlp/commit/5d83f1e8482ca304db8be726cad89554c88f136a, https://huntr.dev/bounties/2f8baf6c-14b3-420d-8ede-9805797cd324	A-STA-CORE-031121/668
strategy11					
formidable_form_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-21	3.5	The Formidable Form Builder â€“ Contact Form, Survey & Quiz Forms Plugin for WordPress plugin before 5.0.07 does not sanitise and escape its Form's Labels, allowing high privileged users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24608**	https://plugins.trac.wordpress.org/changeset/2609911	A-STR-FORM-031121/669
Improper	25-Oct-21	6.8	The Formidable Form	https://githu	A-STR-FORM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Builder WordPress plugin before 4.09.05 allows to inject certain HTML Tags like <audio>,<video>,<img>,<a> and<button>.This could allow an unauthenticated, remote attacker to exploit a HTML-injection byinjecting a malicous link. The HTML-injection may trick authenticated users to follow the link. If the Link gets clicked, Javascript code can be executed. The vulnerability is due to insufficient sanitization of the "data-frmverify" tag for links in the web-based entry inspection page of affected systems. A successful exploitation incomibantion with CSRF could allow the attacker to perform arbitrary actions on an affected system with the privileges of the user. These actions include stealing the users account by changing their password or allowing attackers to submit their own code through an authenticated user resulting in Remote Code Execution. If an authenticated user who is able to edit Wordpress PHP Code in any kind, clicks the malicious link, PHP code can be edited. **CVE ID : CVE-2021-24884**	b.com/Strategy11/formidable-forms/pull/335/files	031121/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Strongswan					
strongswan					
Integer Overflow or Wraparound	18-Oct-21	5	The gmp plugin in strongSwan before 5.9.4 has a remote integer overflow via a crafted certificate with an RSASSA-PSS signature. For example, this can be triggered by an unrelated self-signed CA certificate sent by an initiator. Remote code execution cannot occur. **CVE ID : CVE-2021-41990**	https://www.strongswan.org/blog/2021/10/18/strongswan-vulnerability-(cve-2021-41990).html	A-STR-STRO-031121/671
Integer Overflow or Wraparound	18-Oct-21	5	The in-memory certificate cache in strongSwan before 5.9.4 has a remote integer overflow upon receiving many requests with different certificates to fill the cache and later trigger the replacement of cache entries. The code attempts to select a less-often-used cache entry by means of a random number generator, but this is not done correctly. Remote code execution might be a slight possibility. **CVE ID : CVE-2021-41991**	https://www.strongswan.org/blog/2021/10/18/strongswan-vulnerability-(cve-2021-41991).html	A-STR-STRO-031121/672
sulu					
sulu					
Improper Neutralization of Input During Web Page Generation	21-Oct-21	3.5	Sulu is an open-source PHP content management system based on the Symfony framework. In versions before 1.6.43 are subject to stored cross site scripting	https://github.com/sulu/sulu/security/advisories/GHSA-h58v-g3q6-q9fx,	A-SUL-SULU-031121/673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacks. HTML input into Tag names is not properly sanitized. Only admin users are allowed to create tags. Users are advised to upgrade. **CVE ID : CVE-2021-41169**	https://github.com/sulu/sulu/commit/20007ac70a3af3c9e53a6acb0ef8794b65642445	
synchro					
bulletin_board_system					
Use of Uninitialized Resource	19-Oct-21	5	An issue was discovered in function scanallsubs in src/sbbs3/scansubs.cpp in Synchronet BBS, which may allow attackers to view sensitive information due to an uninitialized value. **CVE ID : CVE-2021-36512**	https://gitlab.synchro.net/main/sbbs/-/issues/276	A-SYN-BULL-031121/674
tammersoft					
shared_files					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	The Easy Download Manager and File Sharing Plugin with frontend file upload â€“ a better Media Library â€” Shared Files WordPress plugin before 1.6.57 does not sanitise and escape some of its settings before outputting them in attributes, which could lead to Stored Cross-Site Scripting issues. **CVE ID : CVE-2021-24736**	N/A	A-TAM-SHAR-031121/675
teamlead					
pdf-light-viewer					
Improper Neutralization of Special Elements	18-Oct-21	9	The WordPress PDF Light Viewer Plugin WordPress plugin before 1.4.12 allows users with Author roles to	N/A	A-TEA-PDF--031121/676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execute arbitrary OS command on the server via OS Command Injection when invoking Ghostscript. **CVE ID : CVE-2021-24684**		
Teamviewer					
teamviewer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of TeamViewer 15.16.8.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TVS files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13697. **CVE ID : CVE-2021-34859**	https://community.teamviewer.com/English/discussion/117794/august-updates-security-patches/p1	A-TEA-TEAM-031121/677
themeum					
tutor_lms					
Improper Neutralization of Input During Web Page Generation ('Cross-site	18-Oct-21	3.5	The Tutor LMS WordPress plugin before 1.9.9 does not escape some of its settings before outputting them in attributes, which could allow high privilege users to perform Cross-Site Scripting	N/A	A-THE-TUTO-031121/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24740**		
thimpress					
learnpress					
Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	21-Oct-21	3.5	The LearnPress WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping on the $custom_profile parameter found in the ~/inc/admin/views/backend-user-profile.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 4.1.3.1. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. Please note that this is seperate from CVE-2021-24702. **CVE ID : CVE-2021-39348**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2614592%40learnpress&new=2614592%40learnpress&sfp_email=&sfph_mail=	A-THI-LEAR-031121/679
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	2.1	The LearnPress WordPress plugin before 4.1.3.1 does not properly sanitize or escape various inputs within course settings, which could allow high privilege users to perform Cross-Site Scripting attacks when the unfiltred_html capability is disallowed **CVE ID : CVE-2021-24702**	N/A	A-THI-LEAR-031121/680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Tibco					
nimbus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-21	3.5	The Web Reporting component of TIBCO Software Inc.'s TIBCO Nimbus contains easily exploitable Stored Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker to social engineer a legitimate user with network access to execute scripts targeting the affected system or the victim's local system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Nimbus: versions 10.4.0 and below. **CVE ID : CVE-2021-35499**	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2021/10/tibco-security-advisory-october-26-2021-tibco-nimbus-2021-35499	A-TIB-NIMB-031121/681
timetracker_project					
timetracker					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	anuko/timetracker is an, open source time tracking system. In affected versions Time Tracker uses browser_today hidden control on a few pages to collect the today's date from user browsers. Because of not checking this parameter for sanity in versions prior to 1.19.30.5601, it was possible to craft an html form with malicious	https://github.com/anuko/timetracker/security/advisories/GHSA-g9cc-m4p4-6xpc	A-TIM-TIME-031121/682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			JavaScript, use social engineering to convince logged on users to execute a POST from such form, and have the attacker-supplied JavaScript to be executed in user's browser. This has been patched in version 1.19.30.5600. Upgrade is recommended. If it is not practical, introduce ttValidDbDateFormatDate function as in the latest version and add a call to it within the access checks block. **CVE ID : CVE-2021-41156**		
Tipsandtricks-hq					
compact_wp_audio_player					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-21	3.5	The Compact WP Audio Player WordPress plugin before 1.9.7 does not escape some of its shortcodes attributes, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2021-24734**	N/A	A-TIP-COMP-031121/683
Cross-Site Request Forgery (CSRF)	18-Oct-21	4.3	The Compact WP Audio Player WordPress plugin before 1.9.7 does not implement nonce checks, which could allow attackers to make a logged in admin change the "Disable Simultaneous Play" setting via a CSRF attack. **CVE ID : CVE-2021-24735**	N/A	A-TIP-COMP-031121/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Trane					
tracer_concierge					
Improper Input Validation	27-Oct-21	6.5	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software. **CVE ID : CVE-2021-38450**	https://us-cert.cisa.gov/ics/advisories/icsa-21-266-02	A-TRA-TRAC-031121/685
Trendmicro					
apex_one					
Incorrect Default Permissions	21-Oct-21	4.6	An incorrect permission assignment vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to load a DLL with escalated privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-42011**	https://success.trendmicro.com/solution/000289229	A-TRE-APEX-031121/686
Out-of-bounds Write	21-Oct-21	4.6	A stack-based buffer overflow vulnerability in Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-APEX-031121/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system in order to exploit this vulnerability. **CVE ID : CVE-2021-42012**		
Uncontrolled Search Path Element	21-Oct-21	4.6	An uncontrolled search path element vulnerabilities in Trend Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar but not identical to CVE-2021-42103. **CVE ID : CVE-2021-42101**	https://success.trendmicro.com/solution/000289229	A-TRE-APEX-031121/688
Uncontrolled Search Path Element	21-Oct-21	4.6	An uncontrolled search path element vulnerabilities in Trend Micro Apex One and Apex One as a Service agents could allow a local attacker to escalate privileges on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-42102**	https://success.trendmicro.com/solution/000289229	A-TRE-APEX-031121/689
Uncontrolled Search Path Element	21-Oct-21	4.6	An uncontrolled search path element vulnerabilities in Trend Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. An	https://success.trendmicro.com/solution/000289229	A-TRE-APEX-031121/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar but not identical to CVE-2021-42101. **CVE ID : CVE-2021-42103**		
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42105, 42106 and 42107. **CVE ID : CVE-2021-42104**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-APEX-031121/691
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-APEX-031121/692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42106 and 42107. **CVE ID : CVE-2021-42105**		
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42105 and 42107. **CVE ID : CVE-2021-42106**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-APEX-031121/693
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-APEX-031121/694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42105 and 42106. **CVE ID : CVE-2021-42107**		
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in the Web Console of Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-42108**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-APEX-031121/695
NULL Pointer Dereference	21-Oct-21	5	A null pointer vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 could allow an attacker to crash the CGI program on affected installations. **CVE ID : CVE-2021-23139**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-APEX-031121/696
worry-free_business_security					
Out-of-bounds Write	21-Oct-21	4.6	A stack-based buffer overflow vulnerability in Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solut	A-TRE-WORR-031121/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-42012**	ion/0002892 29	
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42105, 42106 and 42107. **CVE ID : CVE-2021-42104**	https://succ ess.trendmic ro.com/solut ion/0002892 30, https://succ ess.trendmic ro.com/solut ion/0002892 29	A-TRE-WORR-031121/698
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit	https://succ ess.trendmic ro.com/solut ion/0002892 30, https://succ ess.trendmic ro.com/solut ion/0002892 29	A-TRE-WORR-031121/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42106 and 42107. **CVE ID : CVE-2021-42105**		
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42105 and 42107. **CVE ID : CVE-2021-42106**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-WORR-031121/700
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-WORR-031121/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not identical to CVE-2021-42104, 42105 and 42106. **CVE ID : CVE-2021-42107**		
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in the Web Console of Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-42108**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-WORR-031121/702
NULL Pointer Dereference	21-Oct-21	5	A null pointer vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 could allow an attacker to crash the CGI program on affected installations. **CVE ID : CVE-2021-23139**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-WORR-031121/703
worry-free_business_security_services					
Out-of-bounds Write	21-Oct-21	4.6	A stack-based buffer overflow vulnerability in Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-WORR-031121/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-42012**		
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42105, 42106 and 42107. **CVE ID : CVE-2021-42104**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-WORR-031121/705
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-WORR-031121/706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not identical to CVE-2021-42104, 42106 and 42107. **CVE ID : CVE-2021-42105**		
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42105 and 42107. **CVE ID : CVE-2021-42106**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-WORR-031121/707
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42105 and 42106.	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-WORR-031121/708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-42107		
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in the Web Console of Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-42108**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-WORR-031121/709
NULL Pointer Dereference	21-Oct-21	5	A null pointer vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 could allow an attacker to crash the CGI program on affected installations. **CVE ID : CVE-2021-23139**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	A-TRE-WORR-031121/710
tuzitio					
camaleon_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-21	3.5	In "Camaleon CMS" application, versions 0.0.1 to 2.6.0 are vulnerable to stored XSS, that allows unprivileged application users to store malicious scripts in the comments section of the post. These scripts are executed in a victim's browser when they open the page containing the	https://github.com/owen2345/camaleon-cms/commit/05506e9087bb05282c0bae6ccfe0283d0332ab3c	A-TUZ-CAMA-031121/711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious comment. **CVE ID : CVE-2021-25969**		
Insufficient Session Expiration	20-Oct-21	6.8	Camaleon CMS 0.1.7 to 2.6.0 doesn't terminate the active session of the users, even after the admin changes the user's password. A user that was already logged in, will still have access to the application even after the password was changed. **CVE ID : CVE-2021-25970**	https://github.com/owen2345/camaleon-cms/commit/77e31bc6cdde7c951fba104aebcd5ebb3f02b030	A-TUZ-CAMA-031121/712
N/A	20-Oct-21	4	In Camaleon CMS, versions 2.0.1 to 2.6.0 are vulnerable to an Uncaught Exception. The app's media upload feature crashes permanently when an attacker with a low privileged access uploads a specially crafted .svg file **CVE ID : CVE-2021-25971**	https://github.com/owen2345/camaleon-cms/commit/ab89584ab32b98a0af3d711e3f508a1d048147d2	A-TUZ-CAMA-031121/713
Server-Side Request Forgery (SSRF)	20-Oct-21	4	In Camaleon CMS, versions 2.1.2.0 to 2.6.0, are vulnerable to Server-Side Request Forgery (SSRF) in the media upload feature, which allows admin users to fetch media files from external URLs but fails to validate URLs referencing to localhost or other internal servers. This allows attackers to read files stored in the internal server. **CVE ID : CVE-2021-25972**	https://github.com/owen2345/camaleon-cms/commit/5a252d537411fdd0127714d66c1d76069dc7e190	A-TUZ-CAMA-031121/714
ultimatemember					
jobboardwp					
Improper	19-Oct-21	3.5	The JobBoardWP WordPress	N/A	A-ULT-JOBB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/includes/admin/class-metabox.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.0.7. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. **CVE ID : CVE-2021-39329**		031121/715
vfbpro					
visual_form_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-21	3.5	The Visual Form Builder WordPress plugin before 3.0.4 does not sanitise or escape its Form Name, allowing high privilege users such as admin to set Cross-Site Scripting payload in them, even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24514**	N/A	A-VFB-VISU-031121/716
video_player_for_youtube_project					
video_player_for_youtube					
Improper Neutralization of Input During Web	25-Oct-21	3.5	The Video Player for YouTube WordPress plugin before 1.4 does not sanitise or validate the parameters	N/A	A-VID-VIDE-031121/717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them which will be triggered in the page/s with the embed malicious shortcode **CVE ID : CVE-2021-24414**		
VIM					
vim					
Heap-based Buffer Overflow	19-Oct-21	6.8	vim is vulnerable to Heap-based Buffer Overflow **CVE ID : CVE-2021-3872**	https://github.com/vim/vim/commit/826bfe4bbd7594188e3d74d2539d9707b1c6a14b, https://huntr.dev/bounties/c958013b-1c09-4939-92ca-92f50aa169e8	A-VIM-VIM-031121/718
vm2_project					
vm2					
Improperly Controlled Modification of Dynamically-Determined Object Attributes	18-Oct-21	7.5	This affects the package vm2 before 3.9.4 via a Prototype Pollution attack vector, which can lead to execution of arbitrary code on the host machine. **CVE ID : CVE-2021-23449**	https://github.com/patriksimek/vm2/commit/b4f6e2bd2c4a1ef52fc4483d8e35f28bc4481886, https://security.netapp.com/advisory/ntap-20211029-	A-VM2-VM2-031121/719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				0010/	
Vmware					
vrealize_operations_tenant					
Exposure of Resource to Wrong Sphere	21-Oct-21	5	Releases prior to VMware vRealize Operations Tenant App 8.6 contain an Information Disclosure Vulnerability. **CVE ID : CVE-2021-22034**	https://www.vmware.com/security/advisories/VMSA-2021-0024.html	A-VMW-VREA-031121/720
Webkitgtk					
webkitgtk					
N/A	20-Oct-21	4.6	BubblewrapLauncher.cpp in WebKitGTK and WPE WebKit before 2.34.1 allows a limited sandbox bypass that allows a sandboxed process to trick host processes into thinking the sandboxed process is not confined by the sandbox, by abusing VFS syscalls that manipulate its filesystem namespace. The impact is limited to host services that create UNIX sockets that WebKit mounts inside its sandbox, and the sandboxed process remains otherwise confined. NOTE: this is similar to CVE-2021-41133. **CVE ID : CVE-2021-42762**	https://bugs.webkit.org/show_bug.cgi?id=231479	A-WEB-WEBK-031121/721
wechat_reward_project					
wechat_reward					
Cross-Site Request Forgery (CSRF)	18-Oct-21	4.3	The Wechat Reward WordPress plugin through 1.7 does not sanitise or escape its QR settings, nor	N/A	A-WEC-WECH-031121/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has any CSRF check in place, allowing attackers to make a logged in admin change the settings and perform Cross-Site Scripting attacks. **CVE ID : CVE-2021-24615**		
wp-special-textboxes_project					
wp-special-textboxes					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-21	3.5	The Special Text Boxes WordPress plugin through 5.9.109 does not sanitise or escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed. **CVE ID : CVE-2021-24485**	N/A	A-WP--WP-S-031121/723
wpchill					
check_\\&_log_email					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-21	6.5	The Check & Log Email WordPress plugin before 1.0.3 does not validate and escape the "order" and "orderby" GET parameters before using them in a SQL statement when viewing logs, leading to SQL injections issues **CVE ID : CVE-2021-24774**	N/A	A-WPC-CHEC-031121/724
wpewebkit					
wpe_webkit					
N/A	20-Oct-21	4.6	BubblewrapLauncher.cpp in WebKitGTK and WPE WebKit before 2.34.1 allows a limited sandbox bypass	https://bugs.webkit.org/show_bug.cgi?id=231479	A-WPE-WPE_-031121/725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that allows a sandboxed process to trick host processes into thinking the sandboxed process is not confined by the sandbox, by abusing VFS syscalls that manipulate its filesystem namespace. The impact is limited to host services that create UNIX sockets that WebKit mounts inside its sandbox, and the sandboxed process remains otherwise confined. NOTE: this is similar to CVE-2021-41133. **CVE ID : CVE-2021-42762**		
wpmailster					
wp_mailster					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	4.3	WP Mailster 1.6.18.0 allows XSS when a victim opens a mail server's details in the mst_servers page, for a crafted server_host, server_name, or connection_parameter parameter. **CVE ID : CVE-2021-28975**	N/A	A-WPM-WP_M-031121/726
wp_cookie_choice_project					
wp_cookie_choice					
Cross-Site Request Forgery (CSRF)	18-Oct-21	4.3	The Wp Cookie Choice WordPress plugin through 1.1.0 is lacking any CSRF check when saving its options, and do not escape them when outputting them in attributes. As a result, an attacker could make a logged in admin change them to	N/A	A-WP_-WP_C-031121/727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary values including XSS payloads via a CSRF attack. **CVE ID : CVE-2021-24595**		
wp_debugging_project					
wp_debugging					
Cross-Site Request Forgery (CSRF)	25-Oct-21	4.3	The WP Debugging WordPress plugin before 2.11.0 has its update_settings() function hooked to admin_init and is missing any capability and CSRF checks, as a result, the settings can be updated by unauthenticated users. **CVE ID : CVE-2021-24779**	N/A	A-WP_-WP_D-031121/728
yonyou					
ufida_product_lifecycle_management					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Oct-21	7.5	All versions of yongyou PLM are affected by a command injection issue. UFIDA PLM (Product Life Cycle Management) is a strategic management method. It applies a series of enterprise application systems to support the entire process from conceptual design to the end of product life, and the collaborative creation, distribution, application and management of product information across organizations. Yonyou PLM uses jboss by default, and you can access the management control background without	N/A	A-YON-UFID-031121/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization An attacker can use this vulnerability to gain server permissions. **CVE ID : CVE-2021-41744**		
yop-poll					
yop-poll					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-21	4.3	The YOP Poll WordPress plugin before 6.1.2 does not escape the perpage parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2021-24885**	https://plugins.trac.wordpress.org/changeset/2227747/	A-YOP-YOP--031121/730
zeen101					
leaky_paywall					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-21	3.5	The Leaky Paywall WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via the ~/class.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 4.16.5. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. **CVE ID : CVE-2021-39357**	https://plugins.trac.wordpress.org/changeset/2615195/leaky-paywall/trunk/class.php	A-ZEE-LEAK-031121/731
Zohocorp					
manageengine_applications_manager					
Server-Side	21-Oct-21	6.4	An SSRF issue was	https://ww	A-ZOH-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (SSRF)			discovered in Zoho ManageEngine Applications Manager build 15200. **CVE ID : CVE-2021-35512**	w.manageengine.com/products/applications_manager/, https://www.manageengine.com/products/applications_manager/release-notes.html	MANA-031121/732
Hardware					
Asus					
ux582lr					
Incorrect Default Permissions	18-Oct-21	4.6	ASUSTek ZenBook Pro Due 15 UX582 laptop firmware through 203 has Insecure Permissions that allow attacks by a physically proximate attacker. **CVE ID : CVE-2021-42055**	https://www.asus.com/Static_WebPage/ASUS-Product-Security-Advisory/	H-ASU-UX58-031121/733
Cisco					
asa_5505					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	H-CIS-ASA_-031121/734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**		
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	H-CIS-ASA_-031121/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/736
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	H-CIS-ASA_-031121/738
Improper Enforcement of Message Integrity During Transmission in a	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-	H-CIS-ASA_-031121/739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Communication Channel			allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**	dos-JxYWMJyL	
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	H-CIS-ASA_-031121/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	H-CIS-ASA_-031121/741
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	H-CIS-ASA_-031121/742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**		
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	H-CIS-ASA_-031121/743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
asa_5512-x					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	H-CIS-ASA_-031121/744
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	H-CIS-ASA_-031121/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34790		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/747
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	H-CIS-ASA_-031121/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**		
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	H-CIS-ASA_-031121/749
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security	https://tools.cisco.com/security/center/content/CiscoSecurityAd	H-CIS-ASA_-031121/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**	visory/cisco-sa-asaftd-snmpaccess-M6yOweq3	
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	H-CIS-ASA_-031121/751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**		
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	H-CIS-ASA_-031121/752
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	H-CIS-ASA_-031121/753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**		
asa_5515-x					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	H-CIS-ASA_-031121/754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**		
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	H-CIS-ASA_-031121/755
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-	H-CIS-ASA_-031121/756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	bypass-cpKGqkng	
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/757
Uncontrolled	27-Oct-21	7.8	A vulnerability in the	https://tools.	H-CIS-ASA_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	031121/758
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	H-CIS-ASA_-031121/759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**		
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	H-CIS-ASA_-031121/760
Uncontrolled Resource	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco	https://tools.cisco.com/se	H-CIS-ASA_-031121/761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	H-CIS-ASA_-031121/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2021-40118**		
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	H-CIS-ASA_-031121/763
asa_5525-x					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-	H-CIS-ASA_-031121/764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**	BMxYjm8M	
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	H-CIS-ASA_-031121/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/766
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-	H-CIS-ASA_-031121/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	cpKGqkng	
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	H-CIS-ASA_-031121/768
Improper	27-Oct-21	5	A vulnerability in the TCP	https://tools.	H-CIS-ASA_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Enforcement of Message Integrity During Transmission in a Communication Channel			Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	031121/769
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	H-CIS-ASA_-031121/770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	H-CIS-ASA_-031121/771
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software	https://tools.cisco.com/security/center/content/Cis	H-CIS-ASA_-031121/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	coSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	H-CIS-ASA_-031121/773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**		
asa_5545-x					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	H-CIS-ASA_-031121/774
Improper Handling of Exceptional	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing	https://tools.cisco.com/security/center	H-CIS-ASA_-031121/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**	/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/777
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	H-CIS-ASA_-031121/778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**		
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	H-CIS-ASA_-031121/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network disruption. **CVE ID : CVE-2021-34793**		
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	H-CIS-ASA_-031121/780
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	H-CIS-ASA_-031121/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**		
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	H-CIS-ASA_-031121/782
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-ASA_-031121/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**	sa-asaftd-ikev2-dos-g4cmrr7C	
asa_5555-x					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	H-CIS-ASA_-031121/784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**		
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	H-CIS-ASA_-031121/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/786
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	H-CIS-ASA_-031121/788
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	H-CIS-ASA_-031121/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**		
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	H-CIS-ASA_-031121/790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	H-CIS-ASA_-031121/791
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	H-CIS-ASA_-031121/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**		
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	H-CIS-ASA_-031121/793
asa_5580					
Improper	27-Oct-21	7.8	A vulnerability in the	https://tools.	H-CIS-ASA_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	031121/794
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	H-CIS-ASA_-031121/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/796
Improper	27-Oct-21	5	Multiple vulnerabilities in	https://tools.	H-CIS-ASA_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	031121/797
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	H-CIS-ASA_-031121/798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**		
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	H-CIS-ASA_-031121/799
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	H-CIS-ASA_-031121/800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**	snmpaccess-M6yOweq3	
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	H-CIS-ASA_-031121/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**		
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	H-CIS-ASA_-031121/802
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	H-CIS-ASA_-031121/803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**		
asa_5585-x					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	H-CIS-ASA_-031121/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**		
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	H-CIS-ASA_-031121/805
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	H-CIS-ASA_-031121/807
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security	https://tools.cisco.com/security/center	H-CIS-ASA_-031121/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	H-CIS-ASA_-031121/809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**		
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	H-CIS-ASA_-031121/810
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco	https://tools.cisco.com/security/center/content/Cis	H-CIS-ASA_-031121/811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	coSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	H-CIS-ASA_-031121/812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	H-CIS-ASA_-031121/813
asr_1000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
asr_1000-esp100					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/815
asr_1000-x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
asr_1001					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/817
asr_1001-hx					
Improper Neutralization of Special Elements used in an OS	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAd	H-CIS-ASR_-031121/818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	visory/cisco-sa-sd-wan-rhpbE34A	
asr_1001-hx_r					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/819
asr_1001-x					
Improper Neutralizatio	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN	https://tools.cisco.com/se	H-CIS-ASR_-031121/820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	
asr_1001-x_r					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
asr_1002					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/822
asr_1002-hx					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with root privileges. **CVE ID : CVE-2021-1529**		
asr_1002-hx_r					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/824
asr_1002-x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/825

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
asr_1002-x_r					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/826
asr_1002_fixed_router					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
asr_1004					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/828
asr_1006					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
asr_1006-x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/830
asr_1009-x					
Improper Neutralization of Special Elements used in an OS Command	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-ASR_-031121/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	sa-sd-wan-rhpbE34A	
asr_1013					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ASR_-031121/832
asr_1023					
Improper Neutralization of Special	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an	https://tools.cisco.com/security/center	H-CIS-ASR_-031121/833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	
catalyst_8300-1n1s-4t2x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-CATA-031121/834
catalyst_8300-1n1s-6t					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-CATA-031121/835
catalyst_8300-2n2s-4t2x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-CATA-031121/836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1529		
catalyst_8300-2n2s-6t					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-CATA-031121/837
catalyst_8500					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-CATA-031121/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
catalyst_8500l					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-CATA-031121/839
catalyst_8510csr					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-CATA-031121/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
catalyst_8510msr					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-CATA-031121/841
catalyst_8540csr					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-CATA-031121/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
catalyst_8540msr					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-CATA-031121/843
csr_1000v					
Improper Neutralization of Special Elements used in an OS Command ('OS	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-	H-CIS-CSR_-031121/844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	rhpbE34A	
isr_1000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/845
isr_1100					
Improper Neutralization of Special Elements	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker	https://tools.cisco.com/security/center/content/Cis	H-CIS-ISR_-031121/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	coSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	
isr_1100-4g\\/6g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/847
isr_1100-4p					
Improper	21-Oct-21	6.9	A vulnerability in the CLI of	https://tools.	H-CIS-ISR_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	031121/848
isr_1100-8p					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
isr_1101					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/850
isr_1101-4p					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with root privileges. **CVE ID : CVE-2021-1529**		
isr_1109					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/852
isr_1109-2p					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
isr_1109-4p					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/854
isr_1111x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
isr_1111x-8p					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/856
isr_111x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
isr_1120					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/858
isr_1160					
Improper Neutralization of Special Elements used in an OS Command	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-ISR_-031121/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	sa-sd-wan-rhpbE34A	
isr_4000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/860
isr_4221					
Improper Neutralization of Special	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an	https://tools.cisco.com/security/center	H-CIS-ISR_-031121/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	
isr_4321					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/862
isr_4331					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/863
isr_4351					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1529		
isr_4431					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/865
isr_4451					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
isr_4451-x					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/867
isr_4461					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	H-CIS-ISR_-031121/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**		
ucs_c125_m5					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/869
ucs_c220_m3					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-	H-CIS-UCS_-031121/870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	dos-TZjrFyZh	
ucs_c220_m4					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ucs_c220_m5					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/872
ucs_c225_m6					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**		
ucs_c22_m3					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/874
ucs_c240_m3					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-UCS_-031121/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	sa-imc-gui-dos-TZjrFyZh	
ucs_c240_m5					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34736		
ucs_c240_sd_m5					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/877
ucs_c245_m6					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**		
ucs_c24_m3					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/879
ucs_c260_m2					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller	https://tools.cisco.com/security/center/content/Cis	H-CIS-UCS_-031121/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	coSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	
ucs_c3160					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**		
ucs_c3260					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/882
ucs_c4200					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**		
ucs_c420_m3					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/884
ucs_c460_m2					
Improper Input	21-Oct-21	5	A vulnerability in the web-based management interface	https://tools.cisco.com/se	H-CIS-UCS_-031121/885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	
ucs_c460_m4					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**		
ucs_c480_m5					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/887
ucs_c480_ml_m5					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**		
ucs_c890_m5					
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/889
ucs_s3260					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-Oct-21	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart. The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2021-34736**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh	H-CIS-UCS_-031121/890
commscope					
arris_surfboard_sb8200					
Cross-Site Request Forgery (CSRF)	21-Oct-21	6.8	The administration web interface for the Arris Surfboard SB8200 lacks any protections against cross-site request forgery attacks. This means that an attacker could make configuration changes (such as changing the administrative password) without the consent of the user. **CVE ID : CVE-2021-20120**	N/A	H-COM-ARRI-031121/891
D-link					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dap-2020					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-21	3.3	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the getpage parameter provided to the webproc endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-12103. **CVE ID : CVE-2021-34860**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201	H-D-L-DAP--031121/892
Stack-based Buffer Overflow	25-Oct-21	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the webproc endpoint, which listens on TCP port 80 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201	H-D-L-DAP--031121/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-12104. **CVE ID : CVE-2021-34861**		
Stack-based Buffer Overflow	25-Oct-21	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the var:menu parameter provided to the webproc endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13270. **CVE ID : CVE-2021-34862**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201	H-D-L-DAP--031121/894
Stack-based Buffer Overflow	25-Oct-21	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the var:page parameter provided to the webproc endpoint. The issue results from the lack of	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201	H-D-L-DAP--031121/895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13271. **CVE ID : CVE-2021-34863**		
Emerson					
wireless_1410d_gateway					
Improper Input Validation	22-Oct-21	6.5	The affected product is vulnerable to improper input validation in the restore file. This enables an attacker to provide malicious config files to replace any file on disk. **CVE ID : CVE-2021-38485**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/896
Exposure of Resource to Wrong Sphere	22-Oct-21	4	The affected product is vulnerable to a disclosure of peer username and password by allowing all users access to read global variables. **CVE ID : CVE-2021-42536**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/897
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Oct-21	6.5	The affected product is vulnerable to a parameter injection via passphrase, which enables the attacker to supply uncontrolled input. **CVE ID : CVE-2021-42538**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/898
Missing Authentication for Critical Function	22-Oct-21	6.5	The affected product is vulnerable to a missing permission validation on system backup restore,	https://us-cert.cisa.gov/ics/advisories/icsa-21-	H-EME-WIRE-031121/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which could lead to account take over and unapproved settings change. **CVE ID : CVE-2021-42539**	278-02	
Write-what-where Condition	22-Oct-21	6.5	The affected product is vulnerable to a unsanitized extract folder for system configuration. A low-privileged user can leverage this logic to overwrite the settings and other key functionality. **CVE ID : CVE-2021-42540**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/900
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Oct-21	6.5	The affected product is vulnerable to directory traversal due to mishandling of provided backup folder structure. **CVE ID : CVE-2021-42542**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/901
wireless_1410_gateway					
Improper Input Validation	22-Oct-21	6.5	The affected product is vulnerable to improper input validation in the restore file. This enables an attacker to provide malicious config files to replace any file on disk. **CVE ID : CVE-2021-38485**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/902
Exposure of Resource to Wrong Sphere	22-Oct-21	4	The affected product is vulnerable to a disclosure of peer username and password by allowing all users access to read global variables. **CVE ID : CVE-2021-42536**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/903
Improper	22-Oct-21	6.5	The affected product is	https://us-	H-EME-WIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			vulnerable to a parameter injection via passphrase, which enables the attacker to supply uncontrolled input. **CVE ID : CVE-2021-42538**	cert.cisa.gov/ics/advisories/icsa-21-278-02	031121/904
Missing Authentication for Critical Function	22-Oct-21	6.5	The affected product is vulnerable to a missing permission validation on system backup restore, which could lead to account take over and unapproved settings change. **CVE ID : CVE-2021-42539**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/905
Write-what-where Condition	22-Oct-21	6.5	The affected product is vulnerable to a unsanitized extract folder for system configuration. A low-privileged user can leverage this logic to overwrite the settings and other key functionality. **CVE ID : CVE-2021-42540**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/906
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Oct-21	6.5	The affected product is vulnerable to directory traversal due to mishandling of provided backup folder structure. **CVE ID : CVE-2021-42542**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/907
wireless_1420_gateway					
Improper Input Validation	22-Oct-21	6.5	The affected product is vulnerable to improper input validation in the restore file. This enables an attacker to provide malicious config files to	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			replace any file on disk. **CVE ID : CVE-2021-38485**		
Exposure of Resource to Wrong Sphere	22-Oct-21	4	The affected product is vulnerable to a disclosure of peer username and password by allowing all users access to read global variables. **CVE ID : CVE-2021-42536**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/909
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Oct-21	6.5	The affected product is vulnerable to a parameter injection via passphrase, which enables the attacker to supply uncontrolled input. **CVE ID : CVE-2021-42538**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/910
Missing Authentication for Critical Function	22-Oct-21	6.5	The affected product is vulnerable to a missing permission validation on system backup restore, which could lead to account take over and unapproved settings change. **CVE ID : CVE-2021-42539**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/911
Write-what-where Condition	22-Oct-21	6.5	The affected product is vulnerable to a unsanitized extract folder for system configuration. A low-privileged user can leverage this logic to overwrite the settings and other key functionality. **CVE ID : CVE-2021-42540**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	H-EME-WIRE-031121/912
Improper Limitation of a Pathname to a	22-Oct-21	6.5	The affected product is vulnerable to directory traversal due to mishandling of provided backup folder	https://us-cert.cisa.gov/ics/advisories/icsa-21-	H-EME-WIRE-031121/913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			structure. **CVE ID : CVE-2021-42542**	278-02	
hpe					
superdome_flex					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	4.3	A potential security vulnerability has been identified in HPE Superdome Flex Servers. The vulnerability could be remotely exploited to allow Cross Site Scripting (XSS) because the Session Cookie is missing an HttpOnly Attribute. HPE has provided a firmware update to resolve the vulnerability in HPE Superdome Flex Servers. **CVE ID : CVE-2021-26589**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04199en_us	H-HPE-SUPE-031121/914
superdome_flex_280					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	4.3	A potential security vulnerability has been identified in HPE Superdome Flex Servers. The vulnerability could be remotely exploited to allow Cross Site Scripting (XSS) because the Session Cookie is missing an HttpOnly Attribute. HPE has provided a firmware update to resolve the vulnerability in HPE Superdome Flex Servers. **CVE ID : CVE-2021-26589**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04199en_us	H-HPE-SUPE-031121/915
Huawei					
cloudengine_12800					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	27-Oct-21	3.3	There is a use-after-free (UAF) vulnerability in Huawei products. An attacker may craft specific packets to exploit this vulnerability. Successful exploitation may cause the service abnormal. Affected product versions include:CloudEngine 12800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 5800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 6800 V200R005C10SPC800,V200R005C20SPC800,V200R019C00SPC800;CloudEngine 7800 V200R005C10SPC800,V200R019C00SPC800. **CVE ID : CVE-2021-37122**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211008-01-cloudengine-en	H-HUA-CLOU-031121/916
cloudengine_5800					
Use After Free	27-Oct-21	3.3	There is a use-after-free (UAF) vulnerability in Huawei products. An attacker may craft specific packets to exploit this vulnerability. Successful exploitation may cause the service abnormal. Affected product versions include:CloudEngine 12800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 5800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 6800	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211008-01-cloudengine-en	H-HUA-CLOU-031121/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R005C10SPC800,V200R005C20SPC800,V200R019C00SPC800;CloudEngine 7800 V200R005C10SPC800,V200R019C00SPC800. **CVE ID : CVE-2021-37122**		
cloudengine_6800					
Use After Free	27-Oct-21	3.3	There is a use-after-free (UAF) vulnerability in Huawei products. An attacker may craft specific packets to exploit this vulnerability. Successful exploitation may cause the service abnormal. Affected product versions include:CloudEngine 12800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 5800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 6800 V200R005C10SPC800,V200R005C20SPC800,V200R019C00SPC800;CloudEngine 7800 V200R005C10SPC800,V200R019C00SPC800. **CVE ID : CVE-2021-37122**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211008-01-cloudengine-en	H-HUA-CLOU-031121/918
cloudengine_7800					
Use After Free	27-Oct-21	3.3	There is a use-after-free (UAF) vulnerability in Huawei products. An attacker may craft specific packets to exploit this vulnerability. Successful exploitation may cause the	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211008-	H-HUA-CLOU-031121/919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service abnormal. Affected product versions include:CloudEngine 12800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 5800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 6800 V200R005C10SPC800,V200R005C20SPC800,V200R019C00SPC800;CloudEngine 7800 V200R005C10SPC800,V200R019C00SPC800. **CVE ID : CVE-2021-37122**	01-cloudengine-en	
fusioncube					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Oct-21	5	There is a path traversal vulnerability in Huawei FusionCube 6.0.2.The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. **CVE ID : CVE-2021-37130**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-pathtraversal-en	H-HUA-FUSI-031121/920
imanager_neteco					
Improper Verification	27-Oct-21	9	There is a signature management vulnerability in	https://www.huawei.co	H-HUA-IMAN-031121/921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Cryptographic Signature			some huawei products. An attacker can forge signature and bypass the signature check. During firmware update process, successful exploit this vulnerability can cause the forged system file overwrite the correct system file. Affected product versions include:iManager NetEco V600R010C00CP2001,V600R010C00CP2002,V600R010C00SPC100,V600R010C00SPC110,V600R010C00SPC120,V600R010C00SPC200,V600R010C00SPC210,V600R010C00SPC300;iManager NetEco 6000 V600R009C00SPC100,V600R009C00SPC110,V600R009C00SPC120,V600R009C00SPC190,V600R009C00SPC200,V600R009C00SPC201,V600R009C00SPC202,V600R009C00SPC210. **CVE ID : CVE-2021-37127**	m/en/psirt/security-advisories/huawei-sa-20211020-01-signature-en	
Improper Neutralization of Formula Elements in a CSV File	27-Oct-21	6	There is a CSV injection vulnerability in ManageOne, iManager NetEco and iManager NetEco 6000. An attacker with high privilege may exploit this vulnerability through some operations to inject the CSV files. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject CSV files to the target	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-csv-en	H-HUA-IMAN-031121/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. **CVE ID : CVE-2021-37131**		
imanager_neteco_6000					
Improper Verification of Cryptographic Signature	27-Oct-21	9	There is a signature management vulnerability in some huawei products. An attacker can forge signature and bypass the signature check. During firmware update process, successful exploit this vulnerability can cause the forged system file overwrite the correct system file. Affected product versions include:iManager NetEco V600R010C00CP2001,V600R010C00CP2002,V600R010C00SPC100,V600R010C00SPC110,V600R010C00SPC120,V600R010C00SPC200,V600R010C00SPC210,V600R010C00SPC300;iManager NetEco 6000 V600R009C00SPC100,V600R009C00SPC110,V600R009C00SPC120,V600R009C00SPC190,V600R009C00SPC200,V600R009C00SPC201,V600R009C00SPC202,V600R009C00SPC210. **CVE ID : CVE-2021-37127**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-signature-en	H-HUA-IMAN-031121/923
Improper Neutralization of Formula Elements in a CSV File	27-Oct-21	6	There is a CSV injection vulnerability in ManageOne, iManager NetEco and iManager NetEco 6000. An attacker with high privilege may exploit this vulnerability through some	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-	H-HUA-IMAN-031121/924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations to inject the CSV files. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject CSV files to the target device. **CVE ID : CVE-2021-37131**	01-csv-en	
ips_module					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	H-HUA-IPS_-031121/925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
ngfw_module					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V20	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	H-HUA-NGFW-031121/926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
nip6600					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C2	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	H-HUA-NIP6-031121/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s12700					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a	https://www.huawei.com/en/psirt/security-	H-HUA-S127-031121/928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500	advisories/huawei-sa-20211020-01-outofwrite-en	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s1700					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	H-HUA-S170-031121/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s2700					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	H-HUA-S270-031121/930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s5700					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	H-HUA-S570-031121/931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s6700					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-	H-HUA-S670-031121/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**	en	
s7700					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10S	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	H-HUA-S770-031121/933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s9700					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	H-HUA-S970-031121/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
usg9500					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R02	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	H-HUA-USG9-031121/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
IBM					
flashsystem_9000					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force ID: 206229. **CVE ID : CVE-2021-29873**	https://www.ibm.com/support/pages/node/6497111, https://www.ibm.com/support/pages/node/6507091, https://exchange.xforce.ibmcloud.com	H-IBM-FLAS-031121/936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/vulnerabilities/206229	
flashsystem_9100					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force ID: 206229. **CVE ID : CVE-2021-29873**	https://www.ibm.com/support/pages/node/6497111, https://www.ibm.com/support/pages/node/6507091, https://exchange.xforce.ibmcloud.com/vulnerabilities/206229	H-IBM-FLAS-031121/937
inhandnetworks					
ir615					
Weak Password Requirements	19-Oct-21	7.5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 does not enforce an efficient password policy. This may allow an attacker with obtained user credentials to enumerate passwords and impersonate other application users and perform operations on their behalf. **CVE ID : CVE-2021-38462**	N/A	H-INH-IR61-031121/938
Inadequate Encryption Strength	19-Oct-21	5.8	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 have inadequate encryption strength, which may allow an attacker to intercept the	N/A	H-INH-IR61-031121/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			communication and steal sensitive information or hijack the session. **CVE ID : CVE-2021-38464**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	4.3	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 do not perform sufficient input validation on client requests from the help page. This may allow an attacker to perform a reflected cross-site scripting attack, which could allow an attacker to run code on behalf of the client browser. **CVE ID : CVE-2021-38466**	N/A	H-INH-IR61-031121/940
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 are vulnerable to stored cross-scripting, which may allow an attacker to hijack sessions of users connected to the system. **CVE ID : CVE-2021-38468**	N/A	H-INH-IR61-031121/941
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-21	6.5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 are vulnerable to an attacker using a ping tool to inject commands into the device. This may allow the attacker to remotely run commands on behalf of the device. **CVE ID : CVE-2021-38470**	N/A	H-INH-IR61-031121/942
Improper Restriction of Rendered UI	19-Oct-21	4.3	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870	N/A	H-INH-IR61-031121/943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Layers or Frames			management portal does not contain an X-FRAME-OPTIONS header, which an attacker may take advantage of by sending a link to an administrator that frames the router's management portal and could lure the administrator to perform changes. **CVE ID : CVE-2021-38472**		
Improper Restriction of Excessive Authenticatio n Attempts	19-Oct-21	5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 have has no account lockout policy configured for the login page of the product. This may allow an attacker to execute a brute-force password attack with no time limitation and without harming the normal operation of the user. This could allow an attacker to gain valid credentials for the product interface. **CVE ID : CVE-2021-38474**	N/A	H-INH-IR61-031121/944
Observable Discrepancy	19-Oct-21	5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 authentication process response indicates and validates the existence of a username. This may allow an attacker to enumerate different user accounts. **CVE ID : CVE-2021-38476**	N/A	H-INH-IR61-031121/945
Improper Neutralizatio	19-Oct-21	6.5	InHand Networks IR615 Router's Versions	N/A	H-INH-IR61-031121/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			2.3.0.r4724 and 2.3.0.r4870 are vulnerable to an attacker using a traceroute tool to inject commands into the device. This may allow the attacker to remotely run commands on behalf of the device. **CVE ID : CVE-2021-38478**		
Cross-Site Request Forgery (CSRF)	19-Oct-21	9.3	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 are vulnerable to cross-site request forgery when unauthorized commands are submitted from a user the web application trusts. This may allow an attacker to remotely perform actions on the router's management portal, such as making configuration changes, changing administrator credentials, and running system commands on the router. **CVE ID : CVE-2021-38480**	N/A	H-INH-IR61-031121/947
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 website used to control the router is vulnerable to stored cross-site scripting, which may allow an attacker to hijack sessions of users connected to the system. **CVE ID : CVE-2021-38482**	N/A	H-INH-IR61-031121/948
Unrestricted Upload of File	19-Oct-21	9	InHand Networks IR615 Router's Versions	N/A	H-INH-IR61-031121/949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
with Dangerous Type			2.3.0.r4724 and 2.3.0.r4870 do not have a filter or signature check to detect or prevent an upload of malicious files to the server, which may allow an attacker, acting as an administrator, to upload malicious files. This could result in cross-site scripting, deletion of system files, and remote code execution. **CVE ID : CVE-2021-38484**		
Improper Authorization	19-Oct-21	6	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 cloud portal allows for self-registration of the affected product without any requirements to create an account, which may allow an attacker to have full control over the product and execute code within the internal network to which the product is connected. **CVE ID : CVE-2021-38486**	N/A	H-INH-IR61-031121/950
Juniper					
128_technology_session_smart_router					
Improper Authentication	19-Oct-21	7.5	The usage of an internal HTTP header created an authentication bypass vulnerability (CWE-287), allowing an attacker to view internal files, change settings, manipulate services and execute arbitrary code. This issue affects all Juniper Networks 128 Technology	https://kb.juniper.net/JSA11256	H-JUN-128_-031121/951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Session Smart Router versions prior to 4.5.11, and all versions of 5.0 up to and including 5.0.1. **CVE ID : CVE-2021-31349**		
acx1000					
Improper Input Validation	19-Oct-21	5	An Improper Input Validation vulnerability in Packet Forwarding Engine manager (FXPC) process of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending specific DHCPv6 packets to the device and crashing the FXPC service. Continued receipt and processing of this specific packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms in ACX Series: ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096 devices. Other ACX platforms are not affected from this issue. This issue affects Juniper Networks Junos OS on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096: 18.4 version 18.4R3-S7 and later versions prior to 18.4R3-S8. This issue does not affect: Juniper Networks Junos OS 18.4 versions prior to 18.4R3-S7	https://kb.juniper.net/JSA11241	H-JUN-ACX1-031121/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096. **CVE ID : CVE-2021-31376**		
acx1100					
Improper Input Validation	19-Oct-21	5	An Improper Input Validation vulnerability in Packet Forwarding Engine manager (FXPC) process of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending specific DHCPv6 packets to the device and crashing the FXPC service. Continued receipt and processing of this specific packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms in ACX Series: ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096 devices. Other ACX platforms are not affected from this issue. This issue affects Juniper Networks Junos OS on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096: 18.4 version 18.4R3-S7 and later versions prior to 18.4R3-S8. This issue does not affect: Juniper Networks Junos OS 18.4 versions prior to 18.4R3-S7	https://kb.juniper.net/JSA11241	H-JUN-ACX1-031121/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096. **CVE ID : CVE-2021-31376**		
acx2100					
Improper Input Validation	19-Oct-21	5	An Improper Input Validation vulnerability in Packet Forwarding Engine manager (FXPC) process of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending specific DHCPv6 packets to the device and crashing the FXPC service. Continued receipt and processing of this specific packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms in ACX Series: ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096 devices. Other ACX platforms are not affected from this issue. This issue affects Juniper Networks Junos OS on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096: 18.4 version 18.4R3-S7 and later versions prior to 18.4R3-S8. This issue does not affect: Juniper Networks Junos OS 18.4 versions prior to 18.4R3-S7	https://kb.juniper.net/JSA11241	H-JUN-ACX2-031121/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096. **CVE ID : CVE-2021-31376**		
acx2200					
Improper Input Validation	19-Oct-21	5	An Improper Input Validation vulnerability in Packet Forwarding Engine manager (FXPC) process of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending specific DHCPv6 packets to the device and crashing the FXPC service. Continued receipt and processing of this specific packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms in ACX Series: ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096 devices. Other ACX platforms are not affected from this issue. This issue affects Juniper Networks Junos OS on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096: 18.4 version 18.4R3-S7 and later versions prior to 18.4R3-S8. This issue does not affect: Juniper Networks Junos OS 18.4 versions prior to 18.4R3-S7	https://kb.juniper.net/JSA11241	H-JUN-ACX2-031121/955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096. **CVE ID : CVE-2021-31376**		
acx4000					
Improper Input Validation	19-Oct-21	5	An Improper Input Validation vulnerability in Packet Forwarding Engine manager (FXPC) process of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending specific DHCPv6 packets to the device and crashing the FXPC service. Continued receipt and processing of this specific packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms in ACX Series: ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096 devices. Other ACX platforms are not affected from this issue. This issue affects Juniper Networks Junos OS on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096: 18.4 version 18.4R3-S7 and later versions prior to 18.4R3-S8. This issue does not affect: Juniper Networks Junos OS 18.4 versions prior to 18.4R3-S7	https://kb.juniper.net/JSA11241	H-JUN-ACX4-031121/956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096. **CVE ID : CVE-2021-31376**		
acx500					
Improper Input Validation	19-Oct-21	5	An Improper Input Validation vulnerability in Packet Forwarding Engine manager (FXPC) process of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending specific DHCPv6 packets to the device and crashing the FXPC service. Continued receipt and processing of this specific packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms in ACX Series: ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096 devices. Other ACX platforms are not affected from this issue. This issue affects Juniper Networks Junos OS on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096: 18.4 version 18.4R3-S7 and later versions prior to 18.4R3-S8. This issue does not affect: Juniper Networks Junos OS 18.4 versions prior to 18.4R3-S7	https://kb.juniper.net/JSA11241	H-JUN-ACX5-031121/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096. **CVE ID : CVE-2021-31376**		
acx5048					
Improper Input Validation	19-Oct-21	5	An Improper Input Validation vulnerability in Packet Forwarding Engine manager (FXPC) process of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending specific DHCPv6 packets to the device and crashing the FXPC service. Continued receipt and processing of this specific packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms in ACX Series: ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096 devices. Other ACX platforms are not affected from this issue. This issue affects Juniper Networks Junos OS on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096: 18.4 version 18.4R3-S7 and later versions prior to 18.4R3-S8. This issue does not affect: Juniper Networks Junos OS 18.4 versions prior to 18.4R3-S7	https://kb.juniper.net/JSA11241	H-JUN-ACX5-031121/958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096. **CVE ID : CVE-2021-31376**		
acx5096					
Improper Input Validation	19-Oct-21	5	An Improper Input Validation vulnerability in Packet Forwarding Engine manager (FXPC) process of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending specific DHCPv6 packets to the device and crashing the FXPC service. Continued receipt and processing of this specific packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms in ACX Series: ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096 devices. Other ACX platforms are not affected from this issue. This issue affects Juniper Networks Junos OS on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096: 18.4 version 18.4R3-S7 and later versions prior to 18.4R3-S8. This issue does not affect: Juniper Networks Junos OS 18.4 versions prior to 18.4R3-S7	https://kb.juniper.net/JSA11241	H-JUN-ACX5-031121/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096. **CVE ID : CVE-2021-31376**		
acx710					
Uncontrolled Resource Consumption	19-Oct-21	7.8	An Uncontrolled Resource Consumption vulnerability in the kernel of Juniper Networks JUNOS OS allows an unauthenticated network based attacker to cause 100% CPU load and the device to become unresponsive by sending a flood of traffic to the out-of-band management ethernet port. Continued receipted of a flood will create a sustained Denial of Service (DoS) condition. Once the flood subsides the system will recover by itself. An indication that the system is affected by this issue would be that kernel and netisr process are shown to be using a lot of CPU cycles like in the following example output: user@host> show system processes extensive ... PID USERNAME PRI NICE SIZE RES STATE C TIME WCPU COMMAND 16 root -72 - 0K 304K WAIT 1 839:40 88.96% intr{swi1: netisr 0} 0 root 97 - 0K 160K RUN 1 732:43 87.99% kernel{bcm560xgmac0 que} This issue affects Juniper	https://kb.juniper.net/JSA11230	H-JUN-ACX7-031121/960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks JUNOS OS on EX2300 Series, EX3400 Series, and ACX710: All versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S9; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31368**		
ex2300					
Uncontrolled Resource Consumption	19-Oct-21	2.9	An Uncontrolled Resource Consumption vulnerability in Juniper Networks Junos OS on EX2300, EX3400 and EX4300 Series platforms allows an adjacent attacker sending a stream of layer 2 frames will trigger an Aggregated Ethernet (AE) interface to go down and thereby causing a Denial of Service (DoS). By continuously sending a stream of specific layer 2 frames an attacker will sustain the Denial of Service (DoS) condition. This issue	https://kb.juniper.net/JSA11227	H-JUN-EX23-031121/961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Juniper Networks Junos OS EX4300 Series All versions prior to 15.1R7-S7; 16.1 versions prior to 16.1R7-S8; 17.1 versions prior to 17.1R2-S12; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2. Juniper Networks Junos OS EX3400 and EX4300-MP Series All versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S9, 18.4R3-S7; 19.1 versions prior to 19.1R2-S3, 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2. Juniper		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS EX2300 Series All versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31365**		
Uncontrolled Resource Consumption	19-Oct-21	7.8	An Uncontrolled Resource Consumption vulnerability in the kernel of Juniper Networks JUNOS OS allows an unauthenticated network based attacker to cause 100% CPU load and the device to become unresponsive by sending a flood of traffic to the out-of-band management ethernet port. Continued receipted of a flood will create a sustained Denial of Service (DoS) condition. Once the flood subsides the system will recover by itself. An indication that the system is affected by this issue would be that kernel and netisr process are shown to be	https://kb.juniper.net/JSA11230	H-JUN-EX23-031121/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using a lot of CPU cycles like in the following example output: user@host> show system processes extensive ... PID USERNAME PRI NICE SIZE RES STATE C TIME WCPU COMMAND 16 root -72 - 0K 304K WAIT 1 839:40 88.96% intr{swi1: netisr 0} 0 root 97 - 0K 160K RUN 1 732:43 87.99% kernel{bcm560xgmac0 que} This issue affects Juniper Networks JUNOS OS on EX2300 Series, EX3400 Series, and ACX710: All versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S9; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31368**		
ex2300-c					
Uncontrolled Resource Consumption	19-Oct-21	7.8	An Uncontrolled Resource Consumption vulnerability in the kernel of Juniper Networks JUNOS OS allows	https://kb.juniper.net/JSA11230	H-JUN-EX23-031121/963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated network based attacker to cause 100% CPU load and the device to become unresponsive by sending a flood of traffic to the out-of-band management ethernet port. Continued receipted of a flood will create a sustained Denial of Service (DoS) condition. Once the flood subsides the system will recover by itself. An indication that the system is affected by this issue would be that kernel and netisr process are shown to be using a lot of CPU cycles like in the following example output: user@host> show system processes extensive ... PID USERNAME PRI NICE SIZE RES STATE C TIME WCPU COMMAND 16 root -72 - 0K 304K WAIT 1 839:40 88.96% intr{swi1: netisr 0} 0 root 97 - 0K 160K RUN 1 732:43 87.99% kernel{bcm560xgmac0 que} This issue affects Juniper Networks JUNOS OS on EX2300 Series, EX3400 Series, and ACX710: All versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S9; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31368**		
ex2300m					
Uncontrolled Resource Consumption	19-Oct-21	7.8	An Uncontrolled Resource Consumption vulnerability in the kernel of Juniper Networks JUNOS OS allows an unauthenticated network based attacker to cause 100% CPU load and the device to become unresponsive by sending a flood of traffic to the out-of-band management ethernet port. Continued receipted of a flood will create a sustained Denial of Service (DoS) condition. Once the flood subsides the system will recover by itself. An indication that the system is affected by this issue would be that kernel and netisr process are shown to be using a lot of CPU cycles like in the following example output: user@host> show system processes extensive ... PID USERNAME PRI NICE SIZE RES STATE C TIME WCPU COMMAND 16 root -	https://kb.juniper.net/JSA11230	H-JUN-EX23-031121/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			72 - 0K 304K WAIT 1 839:40 88.96% intr{swi1: netisr 0} 0 root 97 - 0K 160K RUN 1 732:43 87.99% kernel{bcm560xgmac0 que} This issue affects Juniper Networks JUNOS OS on EX2300 Series, EX3400 Series, and ACX710: All versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S9; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31368**		
ex3400					
Uncontrolled Resource Consumption	19-Oct-21	2.9	An Uncontrolled Resource Consumption vulnerability in Juniper Networks Junos OS on EX2300, EX3400 and EX4300 Series platforms allows an adjacent attacker sending a stream of layer 2 frames will trigger an Aggregated Ethernet (AE) interface to go down and thereby causing a Denial of	https://kb.juniper.net/JSA11227	H-JUN-EX34-031121/965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). By continuously sending a stream of specific layer 2 frames an attacker will sustain the Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS EX4300 Series All versions prior to 15.1R7-S7; 16.1 versions prior to 16.1R7-S8; 17.1 versions prior to 17.1R2-S12; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2. Juniper Networks Junos OS EX3400 and EX4300-MP Series All versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S9, 18.4R3-S7; 19.1 versions prior to 19.1R2-S3, 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2. Juniper Networks Junos OS EX2300 Series All versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31365**		
Uncontrolled Resource Consumption	19-Oct-21	7.8	An Uncontrolled Resource Consumption vulnerability in the kernel of Juniper Networks JUNOS OS allows an unauthenticated network based attacker to cause 100% CPU load and the device to become unresponsive by sending a flood of traffic to the out-of-band management ethernet port. Continued receipted of a flood will create a sustained Denial of Service (DoS) condition. Once the	https://kb.juniper.net/JSA11230	H-JUN-EX34-031121/966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flood subsides the system will recover by itself. An indication that the system is affected by this issue would be that kernel and netisr process are shown to be using a lot of CPU cycles like in the following example output: user@host> show system processes extensive ... PID USERNAME PRI NICE SIZE RES STATE C TIME WCPU COMMAND 16 root -72 - 0K 304K WAIT 1 839:40 88.96% intr{swi1: netisr 0} 0 root 97 - 0K 160K RUN 1 732:43 87.99% kernel{bcm560xgmac0 que} This issue affects Juniper Networks JUNOS OS on EX2300 Series, EX3400 Series, and ACX710: All versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S9; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31368**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ex4300					
Uncontrolled Resource Consumption	19-Oct-21	2.9	An Uncontrolled Resource Consumption vulnerability in Juniper Networks Junos OS on EX2300, EX3400 and EX4300 Series platforms allows an adjacent attacker sending a stream of layer 2 frames will trigger an Aggregated Ethernet (AE) interface to go down and thereby causing a Denial of Service (DoS). By continuously sending a stream of specific layer 2 frames an attacker will sustain the Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS EX4300 Series All versions prior to 15.1R7-S7; 16.1 versions prior to 16.1R7-S8; 17.1 versions prior to 17.1R2-S12; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S2,	https://kb.juniper.net/JSA11227	H-JUN-EX43-031121/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.4R2. Juniper Networks Junos OS EX3400 and EX4300-MP Series All versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S9, 18.4R3-S7; 19.1 versions prior to 19.1R2-S3, 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2. Juniper Networks Junos OS EX2300 Series All versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31365**		
ex4300-mp					
Uncontrolled Resource	19-Oct-21	2.9	An Uncontrolled Resource Consumption vulnerability	https://kb.juniper.net/JS	H-JUN-EX43-031121/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			in Juniper Networks Junos OS on EX2300, EX3400 and EX4300 Series platforms allows an adjacent attacker sending a stream of layer 2 frames will trigger an Aggregated Ethernet (AE) interface to go down and thereby causing a Denial of Service (DoS). By continuously sending a stream of specific layer 2 frames an attacker will sustain the Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS EX4300 Series All versions prior to 15.1R7-S7; 16.1 versions prior to 16.1R7-S8; 17.1 versions prior to 17.1R2-S12; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2. Juniper Networks Junos OS EX3400 and EX4300-MP Series All	A11227	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S9, 18.4R3-S7; 19.1 versions prior to 19.1R2-S3, 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2. Juniper Networks Junos OS EX2300 Series All versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31365**		
ex4600					
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS	https://kb.juniper.net/JSA11232	H-JUN-EX46-031121/969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ex4600-vc					
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3;	https://kb.juniper.net/JSA11232	H-JUN-EX46-031121/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
ex4650					
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-	https://kb.juniper.net/JSA11232	H-JUN-EX46-031121/971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
mx10					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3,	https://kb.juniper.net/JSA11216	H-JUN-MX10-031121/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions	https://kb.juniper.net/JSA11228	H-JUN-MX10-031121/973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions	https://kb.juniper.net/JSA11231	H-JUN-MX10-031121/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g.	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	H-JUN-MX10-031121/975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx10000					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**	https://kb.juniper.net/JSA11216	H-JUN-MX10-031121/976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3;	https://kb.juniper.net/JSA11231	H-JUN-MX10-031121/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	H-JUN-MX10-031121/978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx10003					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS	https://kb.juniper.net/JSA11216	H-JUN-MX10-031121/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and	https://kb.juniper.net/JSA11228	H-JUN-MX10-031121/980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial	https://kb.juniper.net/JSA11231	H-JUN-MX10-031121/981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E	https://kb.juniper.net/JS	H-JUN-MX10-031121/982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects:	A11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx10008					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of	https://kb.juniper.net/JSA11216	H-JUN-MX10-031121/983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue	https://kb.juniper.net/JSA11228	H-JUN-MX10-031121/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has	https://kb.juniper.net/JSA11231	H-JUN-MX10-031121/985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-	H-JUN-MX10-031121/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions	configuring.html	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx10016					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8;	https://kb.juniper.net/JSA11216	H-JUN-MX10-031121/987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3	https://kb.juniper.net/JSA11228	H-JUN-MX10-031121/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue	https://kb.juniper.net/JSA11231	H-JUN-MX10-031121/989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	H-JUN-MX10-031121/990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx104					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2;	https://kb.juniper.net/JSA11216	H-JUN-MX10-031121/991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to	https://kb.juniper.net/JSA11228	H-JUN-MX10-031121/992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6;	https://kb.juniper.net/JSA11231	H-JUN-MX10-031121/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 :	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	H-JUN-MX10-031121/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31379		
mx150					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**	https://kb.juniper.net/JSA11216	H-JUN-MX15-031121/995
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of	https://kb.juniper.net/JS	H-JUN-MX15-031121/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**	A11228	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3;	https://kb.juniper.net/JSA11231	H-JUN-MX15-031121/997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	H-JUN-MX15-031121/998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx2008					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS	https://kb.juniper.net/JSA11216	H-JUN-MX20-031121/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and	https://kb.juniper.net/JSA11228	H-JUN-MX20-031121/1000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial	https://kb.juniper.net/JSA11231	H-JUN-MX20-031121/1001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E	https://kb.juniper.net/JS	H-JUN-MX20-031121/1002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects:	A11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx2010					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of	https://kb.juniper.net/JSA11216	H-JUN-MX20-031121/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue	https://kb.juniper.net/JSA11228	H-JUN-MX20-031121/1004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has	https://kb.juniper.net/JSA11231	H-JUN-MX20-031121/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-	H-JUN-MX20-031121/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions	configuring.html	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx2020					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8;	https://kb.juniper.net/JSA11216	H-JUN-MX20-031121/1007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3	https://kb.juniper.net/JSA11228	H-JUN-MX20-031121/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue	https://kb.juniper.net/JSA11231	H-JUN-MX20-031121/1009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	H-JUN-MX20-031121/1010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx204					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2;	https://kb.juniper.net/JSA11216	H-JUN-MX20-031121/1011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to	https://kb.juniper.net/JSA11228	H-JUN-MX20-031121/1012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6;	https://kb.juniper.net/JSA11231	H-JUN-MX20-031121/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 :	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	H-JUN-MX20-031121/1014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31379		
mx240					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**	https://kb.juniper.net/JSA11216	H-JUN-MX24-031121/1015
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of	https://kb.juniper.net/JS	H-JUN-MX24-031121/1016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**	A11228	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3;	https://kb.juniper.net/JSA11231	H-JUN-MX24-031121/1017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	H-JUN-MX24-031121/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx40					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS	https://kb.juniper.net/JSA11216	H-JUN-MX40-031121/1019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and	https://kb.juniper.net/JSA11228	H-JUN-MX40-031121/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial	https://kb.juniper.net/JSA11231	H-JUN-MX40-031121/1021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E	https://kb.juniper.net/JS	H-JUN-MX40-031121/1022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects:	A11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx480					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of	https://kb.juniper.net/JSA11216	H-JUN-MX48-031121/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue	https://kb.juniper.net/JSA11228	H-JUN-MX48-031121/1024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has	https://kb.juniper.net/JSA11231	H-JUN-MX48-031121/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-	H-JUN-MX48-031121/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions	configuring.html	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx5					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8;	https://kb.juniper.net/JSA11216	H-JUN-MX5-031121/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3	https://kb.juniper.net/JSA11228	H-JUN-MX5-031121/1028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue	https://kb.juniper.net/JSA11231	H-JUN-MX5-031121/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	H-JUN-MX5-031121/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
mx80					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2;	https://kb.juniper.net/JSA11216	H-JUN-MX80-031121/1031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to	https://kb.juniper.net/JSA11228	H-JUN-MX80-031121/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6;	https://kb.juniper.net/JSA11231	H-JUN-MX80-031121/1033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 :	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	H-JUN-MX80-031121/1034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31379		
mx960					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7; 19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**	https://kb.juniper.net/JSA11216	H-JUN-MX96-031121/1035
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of	https://kb.juniper.net/JS	H-JUN-MX96-031121/1036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**	A11228	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3;	https://kb.juniper.net/JSA11231	H-JUN-MX96-031121/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	H-JUN-MX96-031121/1038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
ptx1000					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6;		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
Missing Release of Memory after Effective Lifetime	19-Oct-21	2.9	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows an adjacent attacker to cause a Denial of Service (DoS) by sending genuine BGP flowspec packets which cause an FPC heap memory leak. Once having run out of memory the FPC will crash and restart along with a core dump. Continued receipted of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to	https://kb.juniper.net/JSA11229	H-JUN-PTX1-031121/1040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.4R1-S4, 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos Evolved is not affected. **CVE ID : CVE-2021-31367**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	6.8	On PTX1000 System, PTX10002-60C System, after upgrading to an affected release, a Race Condition vulnerability between the chassis daemon (chassisd) and firewall process (dfwd) of Juniper Networks Junos OS, may update the device's interfaces with incorrect firewall filters. This issue only occurs when upgrading the device to an affected version of Junos OS. Interfaces intended to have protections may have no protections assigned to them. Interfaces with one type of protection pattern may have alternate protections assigned to them. Interfaces intended to have no protections may have protections assigned to them. These firewall rule misassignments may allow genuine traffic intended to be stopped at the interface to propagate further, potentially causing	https://kb.juniper.net/JSA11250, https://kb.juniper.net/KB10956	H-JUN-PTX1-031121/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disruptions in services by propagating unwanted traffic. An attacker may be able to take advantage of these misassignments. This issue affects Juniper Networks Junos OS on PTX1000 System: 17.2 versions 17.2R1 and later versions prior to 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R1-S1, 20.4R2. This issue does not affect Juniper Networks Junos OS prior to version 17.2R1 on PTX1000 System. This issue affects Juniper Networks Junos OS on PTX10002-60C System: 18.2 versions 18.2R1 and later versions prior to 18.4 versions prior to 18.4R3-S9; 19.1 versions later than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.1R1 prior to 19.4 versions prior to 19.4R2-S5, 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions 20.4R1 and later versions prior to 21.1 versions prior to 21.1R2; 21.2 versions 21.2R1 and later versions prior to 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS prior to version 18.2R1 on PTX10002-60C System. This issue impacts all filter families (inet, inet6, etc.) and all loopback filters. It does not rely upon the location where a filter is set, impacting both logical and physical interfaces. **CVE ID : CVE-2021-31382**		
ptx1000-72q					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
ptx10000					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
ptx10001					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
ptx10001-36mr					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7,	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
Missing Release of Memory after Effective Lifetime	19-Oct-21	2.9	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows an adjacent attacker to cause a Denial of Service (DoS) by sending genuine BGP flowspec packets which	https://kb.juniper.net/JSA11229	H-JUN-PTX1-031121/1046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause an FPC heap memory leak. Once having run out of memory the FPC will crash and restart along with a core dump. Continued receipted of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos Evolved is not affected. **CVE ID : CVE-2021-31367**		
ptx100016					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
ptx10002					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
Missing Release of Memory after Effective Lifetime	19-Oct-21	2.9	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows an adjacent attacker to cause a Denial of Service (DoS) by sending genuine BGP flowspec packets which cause an FPC heap memory	https://kb.juniper.net/JSA11229	H-JUN-PTX1-031121/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leak. Once having run out of memory the FPC will crash and restart along with a core dump. Continued receipted of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos Evolved is not affected. **CVE ID : CVE-2021-31367**		
ptx10002-60c					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1;		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	6.8	On PTX1000 System, PTX10002-60C System, after upgrading to an affected release, a Race Condition vulnerability between the chassis daemon (chassisd) and firewall process (dfwd) of Juniper Networks Junos OS, may update the device's interfaces with incorrect firewall filters. This issue only occurs when upgrading the device to an affected version of Junos OS. Interfaces intended to have protections may have no protections assigned to them. Interfaces with one type of protection pattern may have alternate protections assigned to them. Interfaces intended to have no protections may have protections assigned to them. These firewall rule misassignments may allow genuine traffic intended to be stopped at the interface to propagate further, potentially causing disruptions in services by propagating unwanted traffic. An attacker may be able to take advantage of	https://kb.juniper.net/JSA11250, https://kb.juniper.net/KB10956	H-JUN-PTX1-031121/1051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these misassignments. This issue affects Juniper Networks Junos OS on PTX1000 System: 17.2 versions 17.2R1 and later versions prior to 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R1-S1, 20.4R2. This issue does not affect Juniper Networks Junos OS prior to version 17.2R1 on PTX1000 System. This issue affects Juniper Networks Junos OS on PTX10002-60C System: 18.2 versions 18.2R1 and later versions prior to 18.4 versions prior to 18.4R3-S9; 19.1 versions later than 19.1R1 prior to 19.4 versions prior to 19.4R2-S5, 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions 20.4R1 and later versions prior to 21.1 versions prior to 21.1R2; 21.2 versions 21.2R1 and later versions prior to 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS prior to version 18.2R1 on PTX10002-60C System. This issue impacts all filter families (inet, inet6, etc.) and all loopback filters. It does not rely upon the location where a filter is set, impacting both logical and physical interfaces. **CVE ID : CVE-2021-31382**		
ptx10003					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4	A Race Condition in the 'show chassis pic' command in Juniper Networks Junos OS Evolved may allow an attacker to crash the port interface concentrator daemon (picd) process on the FPC, if the command is executed coincident with other system events outside the attacker's control, leading to a Denial of Service (DoS) condition. Continued execution of the CLI command, under precise conditions, could create a sustained Denial of Service (DoS) condition. This issue affects all Juniper Networks	https://kb.juniper.net/JSA11212	H-JUN-PTX1-031121/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS Evolved versions prior to 20.1R2-EVO on PTX10003 and PTX10008 platforms. Junos OS is not affected by this vulnerability. **CVE ID : CVE-2021-0298**		
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
Missing Release of Memory after Effective Lifetime	19-Oct-21	2.9	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows an adjacent attacker to cause a Denial of Service (DoS) by sending genuine BGP flowspec packets which cause an FPC heap memory leak. Once having run out of memory the FPC will crash	https://kb.juniper.net/JSA11229	H-JUN-PTX1-031121/1054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and restart along with a core dump. Continued receipted of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos Evolved is not affected. **CVE ID : CVE-2021-31367**		
ptx10003_160c					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
ptx10003_80c					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
ptx10003_81cd					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
ptx10004					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
Missing Release of Memory after Effective Lifetime	19-Oct-21	2.9	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows an adjacent attacker to cause a Denial of Service (DoS) by sending genuine BGP flowspec packets which cause an FPC heap memory	https://kb.juniper.net/JSA11229	H-JUN-PTX1-031121/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leak. Once having run out of memory the FPC will crash and restart along with a core dump. Continued receipted of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos Evolved is not affected. **CVE ID : CVE-2021-31367**		
ptx10008					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4	A Race Condition in the 'show chassis pic' command in Juniper Networks Junos OS Evolved may allow an attacker to crash the port interface concentrator daemon (picd) process on the FPC, if the command is executed coincident with other system events outside the attacker's control, leading to a Denial of Service (DoS) condition. Continued execution of the CLI	https://kb.juniper.net/JSA11212	H-JUN-PTX1-031121/1060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command, under precise conditions, could create a sustained Denial of Service (DoS) condition. This issue affects all Juniper Networks Junos OS Evolved versions prior to 20.1R2-EVO on PTX10003 and PTX10008 platforms. Junos OS is not affected by this vulnerability. **CVE ID : CVE-2021-0298**		
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4;	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
Missing Release of Memory after Effective Lifetime	19-Oct-21	2.9	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows an adjacent attacker to cause a Denial of Service	https://kb.juniper.net/JSA11229	H-JUN-PTX1-031121/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(DoS) by sending genuine BGP flowspec packets which cause an FPC heap memory leak. Once having run out of memory the FPC will crash and restart along with a core dump. Continued receipted of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos Evolved is not affected. **CVE ID : CVE-2021-31367**		
ptx10016					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU	https://kb.juniper.net/JSA11223	H-JUN-PTX1-031121/1063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
Missing Release of Memory after Effective Lifetime	19-Oct-21	2.9	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows an adjacent attacker to cause a Denial of Service (DoS) by sending genuine BGP flowspec packets which cause an FPC heap memory leak. Once having run out of memory the FPC will crash and restart along with a core dump. Continued receipted of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4	https://kb.juniper.net/JSA11229	H-JUN-PTX1-031121/1064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos Evolved is not affected. **CVE ID : CVE-2021-31367**		
ptx3000					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions	https://kb.juniper.net/JSA11223	H-JUN-PTX3-031121/1065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
Missing Release of Memory after Effective Lifetime	19-Oct-21	2.9	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows an adjacent attacker to cause a Denial of Service (DoS) by sending genuine BGP flowspec packets which cause an FPC heap memory leak. Once having run out of memory the FPC will crash	https://kb.juniper.net/JSA11229	H-JUN-PTX3-031121/1066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and restart along with a core dump. Continued receipted of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos Evolved is not affected. **CVE ID : CVE-2021-31367**		
ptx5000					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued	https://kb.juniper.net/JSA11223	H-JUN-PTX5-031121/1067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
Missing Release of Memory after Effective Lifetime	19-Oct-21	2.9	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows an adjacent attacker to cause a Denial of Service (DoS) by sending genuine BGP flowspec packets which cause an FPC heap memory leak. Once having run out of memory the FPC will crash and restart along with a core dump. Continued receipted of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos Evolved is not affected. **CVE ID : CVE-2021-31367**	https://kb.juniper.net/JSA11229	H-JUN-PTX5-031121/1068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qfx10000					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2	https://kb.juniper.net/JSA11223	H-JUN-QFX1-031121/1069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx10002					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained	https://kb.juniper.net/JSA11223	H-JUN-QFX1-031121/1070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx10002-32q					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions	https://kb.juniper.net/JSA11223	H-JUN-QFX1-031121/1071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx10002-60c					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of	https://kb.juniper.net/JSA11223	H-JUN-QFX1-031121/1072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx10002-72q					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions	https://kb.juniper.net/JSA11223	H-JUN-QFX1-031121/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx10008					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending	https://kb.juniper.net/JSA11223	H-JUN-QFX1-031121/1074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx10016					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7,	https://kb.juniper.net/JSA11223	H-JUN-QFX1-031121/1075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx10k					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network	https://kb.juniper.net/JSA11223	H-JUN-QFX1-031121/1076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx3000-g					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3	https://kb.juniper.net/JSA11223	H-JUN-QFX3-031121/1077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx3000-m					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper	https://kb.juniper.net/JSA11223	H-JUN-QFX3-031121/1078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6;		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx3008-i					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1	https://kb.juniper.net/JSA11223	H-JUN-QFX3-031121/1079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx3100					
Improper Check for Unusual or	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability	https://kb.juniper.net/JSA11223	H-JUN-QFX3-031121/1080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx3500					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions	https://kb.juniper.net/JSA11223	H-JUN-QFX3-031121/1081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx3600					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2,	https://kb.juniper.net/JSA11223	H-JUN-QFX3-031121/1082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
qfx3600-i					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS)	https://kb.juniper.net/JSA11223	H-JUN-QFX3-031121/1083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31361		
qfx5100					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-	https://kb.juniper.net/JSA11223	H-JUN-QFX5-031121/1084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS).	https://kb.juniper.net/JSA11232	H-JUN-QFX5-031121/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
N/A	19-Oct-21	5	Juniper Networks Junos OS uses the 128.0.0.0/2 subnet for internal communications between the RE and PFEs. It was discovered that packets utilizing these IP addresses may egress an QFX5110 switch, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet, leading to an information	https://kb.juniper.net/JSA11236	H-JUN-QFX5-031121/1086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposure vulnerability. This issue affects: Juniper Networks Junos OS on QFX5110 Series: All versions prior to 17.3R3-S12; 18.1 versions prior to 18.1R3-S13; 18.3 versions prior to 18.3R3-S5; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2; **CVE ID : CVE-2021-31371**		
qfx5100-96s					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued	https://kb.juniper.net/JSA11223	H-JUN-QFX5-031121/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1	https://kb.juniper.net/JSA11232	H-JUN-QFX5-031121/1088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
qfx5110					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to	https://kb.juniper.net/JSA11223	H-JUN-QFX5-031121/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high	https://kb.juniper.net/JSA11232	H-JUN-QFX5-031121/1090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
N/A	19-Oct-21	5	Juniper Networks Junos OS uses the 128.0.0.0/2 subnet for internal communications between the RE and PFEs. It	https://kb.juniper.net/JSA11236	H-JUN-QFX5-031121/1091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			was discovered that packets utilizing these IP addresses may egress an QFX5110 switch, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet, leading to an information exposure vulnerability. This issue affects: Juniper Networks Junos OS on QFX5110 Series: All versions prior to 17.3R3-S12; 18.1 versions prior to 18.1R3-S13; 18.3 versions prior to 18.3R3-S5; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2; **CVE ID : CVE-2021-31371**		
qfx5120					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows	https://kb.juniper.net/JSA11223	H-JUN-QFX5-031121/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5;	https://kb.juniper.net/JSA11232	H-JUN-QFX5-031121/1093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
N/A	19-Oct-21	5	Juniper Networks Junos OS uses the 128.0.0.0/2 subnet for internal communications between the RE and PFEs. It was discovered that packets utilizing these IP addresses may egress an QFX5110 switch, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet, leading to an information exposure vulnerability. This issue affects: Juniper Networks Junos OS on QFX5110 Series: All versions prior to 17.3R3-S12; 18.1 versions prior to 18.1R3-S13; 18.3 versions prior to 18.3R3-S5; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions	https://kb.juniper.net/JSA11236	H-JUN-QFX5-031121/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2; **CVE ID : CVE-2021-31371**		
qfx5130					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to	https://kb.juniper.net/JSA11223	H-JUN-QFX5-031121/1095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and	https://kb.juniper.net/JSA11232	H-JUN-QFX5-031121/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
qfx5200					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2,	https://kb.juniper.net/JSA11223	H-JUN-QFX5-031121/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of	https://kb.juniper.net/JSA11232	H-JUN-QFX5-031121/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
N/A	19-Oct-21	5	Juniper Networks Junos OS uses the 128.0.0.0/2 subnet for internal communications between the RE and PFEs. It was discovered that packets utilizing these IP addresses may egress an QFX5110 switch, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet, leading to an information exposure vulnerability. This issue affects: Juniper Networks Junos OS on	https://kb.juniper.net/JSA11236	H-JUN-QFX5-031121/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QFX5110 Series: All versions prior to 17.3R3-S12; 18.1 versions prior to 18.1R3-S13; 18.3 versions prior to 18.3R3-S5; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2; **CVE ID : CVE-2021-31371**		
qfx5200-32c					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS)	https://kb.juniper.net/JSA11223	H-JUN-QFX5-031121/1100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31361		
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3;	https://kb.juniper.net/JSA11232	H-JUN-QFX5-031121/1101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
qfx5200-48y					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions	https://kb.juniper.net/JSA11223	H-JUN-QFX5-031121/1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will	https://kb.juniper.net/JSA11232	H-JUN-QFX5-031121/1103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
qfx5210					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX	https://kb.juniper.net/JSA11223	H-JUN-QFX5-031121/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3	https://kb.juniper.net/JSA11232	H-JUN-QFX5-031121/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
N/A	19-Oct-21	5	Juniper Networks Junos OS uses the 128.0.0.0/2 subnet for internal communications between the RE and PFEs. It was discovered that packets utilizing these IP addresses may egress an QFX5110 switch, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet, leading to an information exposure vulnerability. This issue affects: Juniper Networks Junos OS on QFX5110 Series: All versions prior to 17.3R3-S12; 18.1 versions prior to 18.1R3-S13; 18.3 versions prior to 18.3R3-S5; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7,	https://kb.juniper.net/JSA11236	H-JUN-QFX5-031121/1106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2; **CVE ID : CVE-2021-31371**		
qfx5210-64c					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-	https://kb.juniper.net/JSA11223	H-JUN-QFX5-031121/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS	https://kb.juniper.net/JSA11232	H-JUN-QFX5-031121/1108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qfx5220					
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2	https://kb.juniper.net/JSA11223	H-JUN-QFX5-031121/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will	https://kb.juniper.net/JSA11232	H-JUN-QFX5-031121/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
srx100					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active	https://kb.juniper.net/JSA11238	H-JUN-SRX1-031121/1111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx110					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions	https://kb.juniper.net/JSA11238	H-JUN-SRX1-031121/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx1400					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to	https://kb.juniper.net/JSA11238	H-JUN-SRX1-031121/1113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx1500					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and	https://kb.juniper.net/JSA11226	H-JUN-SRX1-031121/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform	https://kb.juniper.net/JSA11238	H-JUN-SRX1-031121/1115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
Missing Authorization	19-Oct-21	7.5	Due to a Missing Authorization weakness and Insufficient Granularity of Access Control in a specific device configuration, a vulnerability exists in Juniper Networks Junos OS on SRX Series whereby an attacker who attempts to access J-Web administrative interfaces can successfully do so from any device interface regardless of the web-management configuration and filter rules which may otherwise protect access to J-Web. This issue affects: Juniper Networks Junos OS SRX Series 20.4 version 20.4R1 and later versions prior to	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252	H-JUN-SRX1-031121/1116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2021-31384**		
srx210					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3.	https://kb.juniper.net/JSA11238	H-JUN-SRX2-031121/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31373		
srx220					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**	https://kb.juniper.net/JSA11238	H-JUN-SRX2-031121/1118
srx240					
Improper Neutralization of Input	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos	https://kb.juniper.net/JSA11238	H-JUN-SRX2-031121/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx240h2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to	https://kb.juniper.net/JSA11238	H-JUN-SRX2-031121/1120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx300					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process,	https://kb.juniper.net/JSA11226	H-JUN-SRX3-031121/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31364		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**	https://kb.juniper.net/JSA11238	H-JUN-SRX3-031121/1122
Missing Authorization	19-Oct-21	7.5	Due to a Missing Authorization weakness and Insufficient Granularity of Access Control in a specific device configuration, a vulnerability exists in	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252	H-JUN-SRX3-031121/1123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS on SRX Series whereby an attacker who attempts to access J-Web administrative interfaces can successfully do so from any device interface regardless of the web-management configuration and filter rules which may otherwise protect access to J-Web. This issue affects: Juniper Networks Junos OS SRX Series 20.4 version 20.4R1 and later versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2021-31384**		
srx320					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which	https://kb.juniper.net/JSA11226	H-JUN-SRX3-031121/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**	https://kb.juniper.net/JSA11238	H-JUN-SRX3-031121/1125
srx340					
Concurrent Execution using Shared Resource with Improper	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper	https://kb.juniper.net/JSA11226	H-JUN-SRX3-031121/1126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior	https://kb.juniper.net/JSA11238	H-JUN-SRX3-031121/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx3400					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**	https://kb.juniper.net/JSA11238	H-JUN-SRX3-031121/1128
srx345					
Concurrent	19-Oct-21	4.3	An Improper Check for	https://kb.ju	H-JUN-SRX3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to	niper.net/JSA11226	031121/1129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to	https://kb.juniper.net/JSA11238	H-JUN-SRX3-031121/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx3600					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions	https://kb.juniper.net/JSA11238	H-JUN-SRX3-031121/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx380					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS	https://kb.juniper.net/JSA11226	H-JUN-SRX3-031121/1132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4	https://kb.juniper.net/JSA11238	H-JUN-SRX3-031121/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx4000					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4	https://kb.juniper.net/JSA11238	H-JUN-SRX4-031121/1134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx4100					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3.	https://kb.juniper.net/JSA11238	H-JUN-SRX4-031121/1135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31373		
Missing Authorization	19-Oct-21	7.5	Due to a Missing Authorization weakness and Insufficient Granularity of Access Control in a specific device configuration, a vulnerability exists in Juniper Networks Junos OS on SRX Series whereby an attacker who attempts to access J-Web administrative interfaces can successfully do so from any device interface regardless of the web-management configuration and filter rules which may otherwise protect access to J-Web. This issue affects: Juniper Networks Junos OS SRX Series 20.4 version 20.4R1 and later versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2021-31384**	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252	H-JUN-SRX4-031121/1136
srx4200					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and	https://kb.juniper.net/JSA11238	H-JUN-SRX4-031121/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
Missing Authorization	19-Oct-21	7.5	Due to a Missing Authorization weakness and Insufficient Granularity of Access Control in a specific device configuration, a vulnerability exists in Juniper Networks Junos OS on SRX Series whereby an attacker who attempts to access J-Web administrative interfaces can successfully do so from any device interface regardless of the web-management configuration and filter rules which may otherwise protect access to J-Web. This	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252	H-JUN-SRX4-031121/1138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue affects: Juniper Networks Junos OS SRX Series 20.4 version 20.4R1 and later versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2021-31384**		
srx4600					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1	https://kb.juniper.net/JSA11238	H-JUN-SRX4-031121/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
Missing Authorization	19-Oct-21	7.5	Due to a Missing Authorization weakness and Insufficient Granularity of Access Control in a specific device configuration, a vulnerability exists in Juniper Networks Junos OS on SRX Series whereby an attacker who attempts to access J-Web administrative interfaces can successfully do so from any device interface regardless of the web-management configuration and filter rules which may otherwise protect access to J-Web. This issue affects: Juniper Networks Junos OS SRX Series 20.4 version 20.4R1 and later versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2021-31384**	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252	H-JUN-SRX4-031121/1140
srx5000					
Concurrent Execution using Shared Resource with	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow	https://kb.juniper.net/JSA11226	H-JUN-SRX5-031121/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2,	https://kb.juniper.net/JSA11238	H-JUN-SRX5-031121/1142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx5400					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX	https://kb.juniper.net/JSA11226	H-JUN-SRX5-031121/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to	https://kb.juniper.net/JSA11238	H-JUN-SRX5-031121/1144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
Missing Authorization	19-Oct-21	7.5	Due to a Missing Authorization weakness and Insufficient Granularity of Access Control in a specific device configuration, a vulnerability exists in Juniper Networks Junos OS on SRX Series whereby an attacker who attempts to access J-Web administrative interfaces can successfully do so from any device interface regardless of the web-management configuration and filter rules which may otherwise protect access to J-Web. This issue affects: Juniper Networks Junos OS SRX Series 20.4 version 20.4R1 and later versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252	H-JUN-SRX5-031121/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS versions prior to 20.4R1. **CVE ID : CVE-2021-31384**		
srx550					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects	https://kb.juniper.net/JSA11226	H-JUN-SRX5-031121/1146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions	https://kb.juniper.net/JSA11238	H-JUN-SRX5-031121/1147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
Missing Authorization	19-Oct-21	7.5	Due to a Missing Authorization weakness and Insufficient Granularity of Access Control in a specific device configuration, a vulnerability exists in Juniper Networks Junos OS on SRX Series whereby an attacker who attempts to access J-Web administrative interfaces can successfully do so from any device interface regardless of the web-management configuration and filter rules which may otherwise protect access to J-Web. This issue affects: Juniper Networks Junos OS SRX Series 20.4 version 20.4R1 and later versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252	H-JUN-SRX5-031121/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4R1. **CVE ID : CVE-2021-31384**		
srx550m					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS	https://kb.juniper.net/JSA11226	H-JUN-SRX5-031121/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4	https://kb.juniper.net/JSA11238	H-JUN-SRX5-031121/1150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx550_hm					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging	https://kb.juniper.net/JSA11226	H-JUN-SRX5-031121/1151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to	https://kb.juniper.net/JSA11238	H-JUN-SRX5-031121/1152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
srx5600					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process,	https://kb.juniper.net/JSA11226	H-JUN-SRX5-031121/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31364		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**	https://kb.juniper.net/JSA11238	H-JUN-SRX5-031121/1154
Missing Authorization	19-Oct-21	7.5	Due to a Missing Authorization weakness and Insufficient Granularity of Access Control in a specific device configuration, a vulnerability exists in	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252	H-JUN-SRX5-031121/1155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS on SRX Series whereby an attacker who attempts to access J-Web administrative interfaces can successfully do so from any device interface regardless of the web-management configuration and filter rules which may otherwise protect access to J-Web. This issue affects: Juniper Networks Junos OS SRX Series 20.4 version 20.4R1 and later versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2021-31384**		
srx5800					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which	https://kb.juniper.net/JSA11226	H-JUN-SRX5-031121/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are: SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**	https://kb.juniper.net/JSA11238	H-JUN-SRX5-031121/1157
Missing Authorization	19-Oct-21	7.5	Due to a Missing Authorization weakness and Insufficient Granularity of Access Control in a specific device configuration, a vulnerability exists in Juniper Networks Junos OS	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252	H-JUN-SRX5-031121/1158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on SRX Series whereby an attacker who attempts to access J-Web administrative interfaces can successfully do so from any device interface regardless of the web-management configuration and filter rules which may otherwise protect access to J-Web. This issue affects: Juniper Networks Junos OS SRX Series 20.4 version 20.4R1 and later versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2021-31384**		
srx650					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to	https://kb.juniper.net/JSA11238	H-JUN-SRX6-031121/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
Microsoft					
surface_pro_3					
Incorrect Authorization	20-Oct-21	3.6	Microsoft Surface Pro 3 Security Feature Bypass Vulnerability **CVE ID : CVE-2021-42299**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42299	H-MIC-SURF-031121/1160
onepeloton					
ttr01					
Incorrect Calculation of Buffer Size	25-Oct-21	5	Incorrect calculation of buffer size vulnerability in Peleton TTR01 up to and including PTV55G allows a remote attacker to trigger a Denial of Service attack through the GymKit daemon process by exploiting a heap overflow in the network server handling the Apple GymKit communication. This can lead to an Apple MFI device not being able to	https://twitter.com/ROPsicle/status/1438216078103044107?s=20	H-ONE-TTR0-031121/1161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticate with the Peleton Bike **CVE ID : CVE-2021-40526**		
Qualcomm					
apq8009					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1162
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1163
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1165
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1167
apq8009w					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1168
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1169
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://www.qualcomm.com/compan	H-QUA-APQ8-031121/1170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
apq8017					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1171
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1172
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1174
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1175
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1983**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1177
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1178
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1179
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-APQ8-031121/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1181
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1182
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1183
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-APQ8-031121/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	r-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1185
apq8037					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1186
apq8053					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-APQ8-031121/1187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	r-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1188
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1189
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1190
Out-of-	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check	https://www.qualcomm.	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	com/company/product-security/bulletins/october-2021-bulletin	031121/1191
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1192
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1194
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1195
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1196
Out-of-	20-Oct-21	7.2	Possible stack overflow due to improper validation of	https://www.qualcomm.	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	com/company/product-security/bulletins/october-2021-bulletin	031121/1197
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1198
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1199
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1201
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1202
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1203
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length	https://www.qualcomm.com/compan	H-QUA-APQ8-031121/1204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	y/product-security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1205
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1206
apq8064au					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided	https://www.qualcomm.com/compan	H-QUA-APQ8-031121/1207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	y/product-security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1208
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1209
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-APQ8-031121/1210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1211
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1212
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-APQ8-031121/1213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1214
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1215
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1216
apq8096au					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null	https://www.qualcomm.	H-QUA-APQ8-031121/1217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	com/company/product-security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1218
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1219
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-APQ8-031121/1220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1221
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1222
Buffer Copy without Checking Size	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing	https://www.qualcomm.com/compan	H-QUA-APQ8-031121/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1224
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1225
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1227
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1228
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-APQ8-031121/1229
Improper Input	20-Oct-21	5	Possible buffer overflow due to Improper validation of	https://www.qualcomm.	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	com/company/product-security/bulletins/october-2021-bulletin	031121/1230
aqt1000					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1231
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1232
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with	https://www.qualcomm.com/company/product-security/bull	H-QUA-AQT1-031121/1233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	etins/octobe r-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-AQT1-031121/1234
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-AQT1-031121/1235
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe	H-QUA-AQT1-031121/1236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1237
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1238
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-AQT1-031121/1239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1240
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1241
Buffer Copy without	20-Oct-21	7.2	Possible buffer overflow due to improper handling of	https://www.qualcomm.	H-QUA-AQT1-031121/1242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	com/company/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1243
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1244
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30256		
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1246
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1247
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1248
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of	https://www.qualcomm.	H-QUA-AQT1-031121/1249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1250
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1251
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AQT1-031121/1253
ar8031					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1254
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-AR80-031121/1255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1256
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1257
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to	https://www.qualcomm.com/company/product-	H-QUA-AR80-031121/1258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1259
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1261
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1262
Improper Restriction of Operations within the	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence	https://www.qualcomm.com/company/product-	H-QUA-AR80-031121/1263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	security/bulletins/october-2021-bulletin	
ar8035					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1264
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1265
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of	https://www.qualcomm.	H-QUA-AR80-031121/1266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	com/company/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1267
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1268
Exposure of Resource to Wrong	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to	https://www.qualcomm.com/compan	H-QUA-AR80-031121/1269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	y/product-security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1270
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1271

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1272
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR80-031121/1273
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-AR80-031121/1274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	etins/octobe r-2021-bulletin	
Improper Authenticatio n	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-AR80-031121/1275
ar9380					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-AR93-031121/1276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR93-031121/1277
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-AR93-031121/1278
csr6030					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://www.qualcomm.com/compan	H-QUA-CSR6-031121/1279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
csr8811					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSR8-031121/1280
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSR8-031121/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSR8-031121/1282
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSR8-031121/1283
csra6620					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while	https://www.qualcomm.com/compan	H-QUA-CSRA-031121/1284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1285
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1286
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to	https://www.qualcomm.com/company/product-	H-QUA-CSRA-031121/1287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1288
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1290
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1291
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-CSRA-031121/1292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	etins/october-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1293
csra6640					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1294
Buffer Copy without Checking Size of Input	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in	https://www.qualcomm.com/company/product-	H-QUA-CSRA-031121/1295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1296
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1297
Exposure of Resource to Wrong	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to	https://www.qualcomm.com/compan	H-QUA-CSRA-031121/1298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1299
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1301
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRA-031121/1302
Improper Restriction of Operations	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check	https://www.qualcomm.com/compan	H-QUA-CSRA-031121/1303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	y/product-security/bulletins/october-2021-bulletin	
csrb31024					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRB-031121/1304
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRB-031121/1305
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in	https://www.qualcomm.com/company/product-security/bull	H-QUA-CSRB-031121/1306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRB-031121/1307
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRB-031121/1308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-CSRB-031121/1309
fsm10055					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1310
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1312
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1313
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1315
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1316
Improper Restriction of Operations within the	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence	https://www.qualcomm.com/company/product-	H-QUA-FSM1-031121/1317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	security/bulletins/october-2021-bulletin	
fsm10056					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1318
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1319
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-FSM1-031121/1320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1321
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1322
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-FSM1-031121/1323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1324
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-FSM1-031121/1325
ipq4018					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check	https://www.qualcomm.	H-QUA-IPQ4-031121/1326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ4-031121/1327
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ4-031121/1328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
ipq4019					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ4-031121/1329
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ4-031121/1330
ipq4028					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ4-031121/1331
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ4-031121/1332
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ4-031121/1333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
ipq4029					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ4-031121/1334
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ4-031121/1335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ4-031121/1336
ipq5010					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ5-031121/1337
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-IPQ5-031121/1338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ5-031121/1339
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ5-031121/1340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30312**		
ipq5018					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ5-031121/1341
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ5-031121/1342
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user	https://www.qualcomm.com/compan	H-QUA-IPQ5-031121/1343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	y/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ5-031121/1344
ipq5028					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ5-031121/1345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ5-031121/1346
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ5-031121/1347
Improper	20-Oct-21	5	Improper authentication of	https://ww	H-QUA-IPQ5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/1348
ipq6000					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1349
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-IPQ6-031121/1350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1351
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
ipq6005					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1353
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1354
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information	https://www.qualcomm.com/company/product-	H-QUA-IPQ6-031121/1355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	security/bulletins/october-2021-bulletin	
ipq6010					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1356
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1358
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1359
ipq6018					
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	H-QUA-IPQ6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/1360
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1361
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1363
ipq6028					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1365
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ6-031121/1366
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-IPQ6-031121/1367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
ipq8064					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1368
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1370
ipq8065					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1371
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to	https://www.qualcomm.com/compan	H-QUA-IPQ8-031121/1372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	y/product-security/bulletins/october-2021-bulletin	
ipq8068					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1373
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
ipq8069					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1375
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq8070					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1377
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1378
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-031121/1379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	etins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1380
ipq8070a					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1382
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1383
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to	https://www.qualcomm.com/compan	H-QUA-IPQ8-031121/1384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	y/product-security/bulletins/october-2021-bulletin	
ipq8071					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1385
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1387
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq8071a					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1389
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1390
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-031121/1391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	etins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1392
ipq8072					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1394
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1395
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to	https://www.qualcomm.com/compan	H-QUA-IPQ8-031121/1396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	y/product-security/bulletins/october-2021-bulletin	
ipq8072a					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1397
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1399
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq8074					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1401
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1402
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-031121/1403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	etins/octobe r-2021-bulletin	
Improper Authenticatio n	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-IPQ8-031121/1404
ipq8074a					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-IPQ8-031121/1405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1406
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1407
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to	https://www.qualcomm.com/compan	H-QUA-IPQ8-031121/1408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	y/product-security/bulletins/october-2021-bulletin	
ipq8076					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1409
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1411
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq8076a					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1413
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1414
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-031121/1415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	etins/octobe r-2021-bulletin	
Improper Authenticatio n	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-IPQ8-031121/1416
ipq8078					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-IPQ8-031121/1417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1418
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1419
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to	https://www.qualcomm.com/compan	H-QUA-IPQ8-031121/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	y/product-security/bulletins/october-2021-bulletin	
ipq8078a					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1421
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1423
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq8173					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1425
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1426
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-031121/1427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	etins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1428
ipq8174					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1430
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-IPQ8-031121/1431
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to	https://www.qualcomm.com/compan	H-QUA-IPQ8-031121/1432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	y/product-security/bulletins/october-2021-bulletin	
mdm8207					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM8-031121/1433
mdm9150					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1435
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1436
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1438
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1439
mdm9206					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-MDM9-031121/1440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1441
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1442
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-MDM9-031121/1443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1444
mdm9207					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1445
mdm9230					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of	https://www.qualcomm.	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	com/company/product-security/bulletins/october-2021-bulletin	031121/1446
mdm9250					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1447
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1448
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption	https://www.qualcomm.com/company/product-	H-QUA-MDM9-031121/1449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1450
mdm9330					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1451
mdm9607					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1452
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1453
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1455
mdm9626					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1456
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1458
mdm9628					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1459
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1461
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1462
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM9-031121/1463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	etins/octobe r-2021-bulletin	
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-MDM9-031121/1464
mdm9630					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-MDM9-031121/1465
mdm9640					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-MDM9-031121/1466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1467
mdm9650					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1468
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1470
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1471
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM9-031121/1472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	etins/october-2021-bulletin	
mdm9655					
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MDM9-031121/1473
msm8108					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1474
msm8208					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of	https://www.qualcomm.	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	com/company/product-security/bulletins/october-2021-bulletin	031121/1475
msm8209					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1476
msm8608					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1477
msm8909w					
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	MSM8-031121/1478
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1479
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1480
msm8917					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-MSM8-031121/1481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	etins/octobe r-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-MSM8-031121/1482
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-MSM8-031121/1483
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-MSM8-031121/1484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1485
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1486
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1487
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-MSM8-031121/1488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1489
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1490
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1491
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-MSM8-031121/1492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1493
msm8920					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1494
msm8937					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1496
msm8940					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1497
msm8953					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1498
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided	https://www.qualcomm.com/compan	H-QUA-MSM8-031121/1499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	y/product-security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1500
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1501
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1503
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1504
Buffer Copy without Checking Size of Input	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in	https://www.qualcomm.com/company/product-	H-QUA-MSM8-031121/1505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1506
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1507
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1508
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR	https://www.qualcomm.com/compan	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	y/product-security/bulletins/october-2021-bulletin	031121/1509
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1510
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1511
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1513
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1514
msm8976					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1515
msm8976sg					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1516
msm8996au					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1517
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1518
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-031121/1519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1520
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1522
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1523
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1524
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-MSM8-031121/1525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1526
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1527
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30292**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1529
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-MSM8-031121/1530
pm8937					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-PM89-031121/1531
pmp8074					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-PMP8-031121/1532
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-PMP8-031121/1533
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-PMP8-031121/1534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-PMP8-031121/1535
qca1023					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA1-031121/1536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
qca1062					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA1-031121/1537
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA1-031121/1538
Improper Authenticatio	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames	https://www.qualcomm.	H-QUA-QCA1-031121/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	com/company/product-security/bulletins/october-2021-bulletin	
qca1064					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA1-031121/1540
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA1-031121/1541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA1-031121/1542
qca10901					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA1-031121/1543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA1-031121/1544
qca1990					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA1-031121/1545
qca2062					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA2-031121/1546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1547
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30302		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1549
qca2064					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1550
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1552
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1553
qca2065					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA2-031121/1554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1555
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30302		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1557
qca2066					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1558
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1560
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA2-031121/1561
qca4010					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA4-031121/1562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	bulletin	
qca4020					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA4-031121/1563
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA4-031121/1564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA4-031121/1565
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA4-031121/1566
qca4024					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA4-031121/1567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA4-031121/1568
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA4-031121/1569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30302		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA4-031121/1570
qca4531					
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA4-031121/1571
qca6174					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	bulletin	
qca6174a					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1573
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1574
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1949		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1576
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1577
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1579
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1580
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1582
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1583
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30316		
qca6175a					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1585
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1586
qca6310					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1588
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1589
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1591
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1592
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1594
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1595
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30288		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1597
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1598
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1599
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1601
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1602
qca6320					
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/1603
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1604
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1605
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-031121/1606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1607
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1608
Buffer Copy without	20-Oct-21	7.2	Possible buffer overflow due to improper validation of	https://www.qualcomm.	H-QUA-QCA6-031121/1609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1610
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1611
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1613
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1614
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1615
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-031121/1616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	etins/october-2021-bulletin	
qca6330					
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1617
qca6335					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1619
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1620
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1622
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1623
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1625
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1626
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1627
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of	https://www.qualcomm.	H-QUA-QCA6-031121/1628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1629
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1630
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1632
qca6390					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1633
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	security/bulletins/october-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1635
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1636
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1638
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1639
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1641
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1642
Buffer Copy without Checking Size of Input	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1644
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1645
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1647
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1648
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1649
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory	https://www.qualcomm.com/compan	H-QUA-QCA6-031121/1650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1651
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1652
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1654
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1655
qca6391					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1657
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1658
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1659
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1661
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1662
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-031121/1663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	etins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1664
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1666
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1667
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1668
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/1669
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1670
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1671
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1673
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1674
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1675
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	H-QUA-QCA6-031121/1676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1677
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1678
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile **CVE ID : CVE-2021-30306**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1680
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1681
qca6420					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1683
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1684
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1686
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1687
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1688
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1690
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1692
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1693
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1694
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/1695
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1696
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1697
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1699
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1700
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1701
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	H-QUA-QCA6-031121/1702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1703
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
qca6421					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1705
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1706
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1707
Out-of-	20-Oct-21	7.2	Possible memory corruption	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/1708
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1709
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1711
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1712
qca6426					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1714
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1715
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1717
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1718
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1720
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1721
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-031121/1722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-QCA6-031121/1723
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-QCA6-031121/1724
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-QCA6-031121/1725
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-security/bull	H-QUA-QCA6-031121/1726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1727
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1728
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1730
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1731
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qca6428					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1733
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1735
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1736
qca6430					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	bulletin	
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1738
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1739
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1936**		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1741
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1742
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1743
Out-of-	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check	https://www.qualcomm.	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	com/company/product-security/bulletins/october-2021-bulletin	031121/1744
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1745
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1969		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1747
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1748
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1750
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1751
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1752
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1754
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1755
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1756
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	H-QUA-QCA6-031121/1757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1758
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
qca6431					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1760
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1761
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1762
Out-of-	20-Oct-21	7.2	Possible memory corruption	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/1763
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1764
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1766
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1767
qca6436					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1769
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1770
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1772
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1773
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1775
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1776
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-031121/1777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-QCA6-031121/1778
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-QCA6-031121/1779
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-QCA6-031121/1780
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-security/bull	H-QUA-QCA6-031121/1781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1782
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1783
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1785
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1786
qca6438					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE	https://www.qualcomm.com/compan	H-QUA-QCA6-031121/1787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1788
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1790
qca6564					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1791
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1793
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1794
qca6564a					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1796
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1797
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1799
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1800
Buffer Copy	20-Oct-21	7.2	Possible buffer overflow due	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/1801
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1802
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1803
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30258**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1805
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1806
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1807
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-031121/1808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1809
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1810
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**		
qca6564au					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1812
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1813
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1949		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1815
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1816
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1818
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1819
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1821
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1822
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1824
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1825
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1826
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-031121/1827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1828
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1829
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**		
qca6574					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1831
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1832
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1833
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://www.qualcomm.com/compan	H-QUA-QCA6-031121/1834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1835
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1836
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1838
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1840
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1841
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-031121/1842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	etins/octobe r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1843
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1844
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30312**		
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1846
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1847
qca6574a					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1848
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in	https://www.qualcomm.com/compan	H-QUA-QCA6-031121/1849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	y/product-security/bulletins/october-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1850
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1851
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1853
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1854
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1856
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1857
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1859
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1860
Buffer Copy without Checking Size	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing	https://www.qualcomm.com/compan	H-QUA-QCA6-031121/1861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1862
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1863
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1865
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1866
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1867
Improper Input	20-Oct-21	4.6	Possible out of bound access due to lack of validation of	https://www.qualcomm.	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	com/company/product-security/bulletins/october-2021-bulletin	031121/1868
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1869
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1870
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1872
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1873
qca6574au					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1875
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1876
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1877
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1879
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1880
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1882
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1883
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1885
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1887
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1888
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1889
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1891
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30297		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1894
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1895
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1896
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1898
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1899
qca6584					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
qca6584au					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1901
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1902
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1904
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1905
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA6-031121/1906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1907
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1909
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1910
qca6595					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1912
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1913
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1914
Integer Overflow or	20-Oct-21	7.2	Possible integer overflow due to improper check of	https://www.qualcomm.	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	com/company/product-security/bulletins/october-2021-bulletin	031121/1915
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1916
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1917
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-031121/1918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	r-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1919
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1920
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation	https://www.qualcomm.	H-QUA-QCA6-031121/1921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1922
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1924
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1925
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1926
qca6595au					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1927
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1928
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1929
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/1930
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1931
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1932
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-031121/1933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1934
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1935
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-031121/1936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1937
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1939
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1940
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1941
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1943
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1944
Improper Restriction of Operations within the Bounds of a Memory	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA6-031121/1945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	r-2021-bulletin	
qca6694					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1946
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1947
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-031121/1948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	etins/october-2021-bulletin	
qca6694au					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1949
qca6696					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1951
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1952
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1953
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1955
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1956
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1958
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1959
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1961
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1963
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1964
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1965
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-031121/1966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	security/bulletins/october-2021-bulletin	
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1967
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA6-031121/1968
qca7500					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA7-031121/1969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA7-031121/1970
qca8072					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1972
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1973
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in	https://www.qualcomm.com/company/product-	H-QUA-QCA8-031121/1974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	security/bulletins/october-2021-bulletin	
qca8075					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1975
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1977
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1978
qca8081					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1979
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1980
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA8-031121/1981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1982
qca8337					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1983
Out-of-	20-Oct-21	7.2	Possible memory corruption	https://ww	H-QUA-QCA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/1984
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1985
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1986
Exposure of Resource to	20-Oct-21	2.1	Improper validation of kernel buffer address while	https://www.qualcomm.	H-QUA-QCA8-031121/1987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	com/company/product-security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1988
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1990
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA8-031121/1991
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA8-031121/1992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
qca9367					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/1993
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/1994
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery	https://www.qualcomm.com/company/product-	H-QUA-QCA9-031121/1995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/1996
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/1997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30310		
qca9369					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/1998
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/1999
qca9377					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA9-031121/2000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	r-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2001
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2002
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2004
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2005
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCA9-031121/2006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2007
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2008
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30310		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2010
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2011
qca9379					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2013
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2014
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2016
qca9531					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2017
qca9558					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2018
qca9561					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2019
qca9563					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-031121/2020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	etins/october-2021-bulletin	
qca9880					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2021
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qca9882					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2023
qca9886					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2025
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2026
qca9887					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
qca9888					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2028
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2030
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2031
qca9889					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-031121/2032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2033
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2035
qca9896					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2036
qca9898					
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	H-QUA-QCA9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/2037
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2038
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qca9980					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2040
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2041
Improper	20-Oct-21	5	Improper authentication of	https://ww	H-QUA-QCA9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/2042
qca9982					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2043
qca9984					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCA9-031121/2044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	r-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2045
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2047
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2048
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qca9985					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2050
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30312**		
qca9990					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2052
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2053
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-031121/2054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	etins/october-2021-bulletin	
qca9992					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2055
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2057
qca9994					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2058
Improper Authenticatio	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames	https://www.qualcomm.	H-QUA-QCA9-031121/2059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCA9-031121/2060
qcm2290					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**		
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2062
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2063
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2065
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2066
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1984**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2068
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2069
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2070
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCM2-031121/2071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30258**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2072
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2073
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2075
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2076
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM2-031121/2077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
qcm4290					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2078
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2079
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1936**		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2081
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2082
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2084
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2085
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCM4-031121/2086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	etins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2087
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2088
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2089
Out-of-	20-Oct-21	7.2	Possible out of bound read or write in VR service due to	https://www.qualcomm.	H-QUA-QCM4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	com/company/product-security/bulletins/october-2021-bulletin	031121/2090
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2091
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2092
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCM4-031121/2093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2094
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2095
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM4-031121/2096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qcm6125					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2097
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2098
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2100
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2101
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1968		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2103
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2104
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2106
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2107
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1985		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2109
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2110
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2111
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2113
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2114
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2116
qcm6490					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2117
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2119
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2120
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2121
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCM6-031121/2122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2123
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2124
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2125
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCM6-031121/2126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2127
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2128
Improper Input	20-Oct-21	4.6	Possible out of bound access due to lack of validation of	https://www.qualcomm.	H-QUA-QCM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	com/company/product-security/bulletins/october-2021-bulletin	031121/2129
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2130
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2131
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCM6-031121/2132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**		
qcn5021					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2133
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2134
Improper Authenticatio	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames	https://www.qualcomm.	H-QUA-QCN5-031121/2135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2136
qcn5022					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2138
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2140
qcn5024					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2141
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN5-031121/2142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2143
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30312**		
qcn5052					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2145
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2146
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user	https://www.qualcomm.com/compan	H-QUA-QCN5-031121/2147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	y/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2148
qcn5054					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2150
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2151
Improper	20-Oct-21	5	Improper authentication of	https://ww	H-QUA-QCN5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/2152
qcn5064					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2153
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCN5-031121/2154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2155
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
qcn5121					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2157
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2158
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information	https://www.qualcomm.com/company/product-	H-QUA-QCN5-031121/2159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	security/bulletins/october-2021-bulletin	
qcn5122					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2160
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2162
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2163
qcn5124					
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	H-QUA-QCN5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/2164
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2165
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2167
qcn5152					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2169
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2170
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN5-031121/2171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
qcn5154					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2172
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2174
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2175
qcn5164					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check	https://www.qualcomm.	H-QUA-QCN5-031121/2176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2177
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2179
qcn5500					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcn5502					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2181
qcn5550					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2182
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN5-031121/2183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	etins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2184
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN5-031121/2185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qcn6023					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN6-031121/2186
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN6-031121/2187
Improper Authenticatio	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames	https://www.qualcomm.	H-QUA-QCN6-031121/2188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN6-031121/2189
qcn6024					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN6-031121/2190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN6-031121/2191
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN6-031121/2192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN6-031121/2193
qcn6122					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN6-031121/2194
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCN6-031121/2195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN6-031121/2196
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN6-031121/2197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30312**		
qcn7605					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN7-031121/2198
qcn7606					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN7-031121/2199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcn9000					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2200
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2201
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN9-031121/2202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	etins/octobe r-2021-bulletin	
Improper Authenticatio n	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-QCN9-031121/2203
qcn9012					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-QCN9-031121/2204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2205
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2206
qcn9022					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE	https://www.qualcomm.com/compan	H-QUA-QCN9-031121/2207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2208
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2210
qcn9024					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2211
Out-of-	20-Oct-21	7.2	Possible stack overflow due	https://ww	H-QUA-QCN9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/2212
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2213
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qcn9070					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2215
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2217
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2218
qcn9072					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN9-031121/2219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2220
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2222
qcn9074					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2223
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV	https://www.qualcomm.com/compan	H-QUA-QCN9-031121/2224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	y/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2225
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qcn9100					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2227
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2229
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCN9-031121/2230
qcs2290					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCS2-031121/2231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2232
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2233
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCS2-031121/2234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2235
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2236
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCS2-031121/2237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2238
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2239
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2240
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCS2-031121/2241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2242
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2243
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30292**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2245
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2246
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS2-031121/2247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qcs405					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2248
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2249
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCS4-031121/2250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2251
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2252
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCS4-031121/2253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2254
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2255
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check	https://www.qualcomm.	H-QUA-QCS4-031121/2256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2257
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2259
qcs410					
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2260
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in	https://www.qualcomm.com/company/product-	H-QUA-QCS4-031121/2261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2262
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2263
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2265
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2266
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption	https://www.qualcomm.com/company/product-	H-QUA-QCS4-031121/2267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2268
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2270
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2271
qcs4290					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCS4-031121/2272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	r-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2273
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2274
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCS4-031121/2275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2276
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2277
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCS4-031121/2278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2279
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2280
Buffer Copy without	20-Oct-21	7.2	Possible buffer overflow due to improper validation of	https://www.qualcomm.	H-QUA-QCS4-031121/2281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2282
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2283
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2285
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2286
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2287
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of	https://www.qualcomm.	H-QUA-QCS4-031121/2288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	com/company/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2289
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS4-031121/2290
qcs603					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided	https://www.qualcomm.com/compan	H-QUA-QCS6-031121/2291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	y/product-security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2292
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2293
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2295
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2296
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1985		
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2298
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2299
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2300
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**		
qcs605					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2302
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2303
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2305
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2306
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1983**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2308
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2309
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2310
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCS6-031121/2311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2312
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2313
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30291		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2315
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2316
qcs610					
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2318
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2319
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2320
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS6-031121/2321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2322
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2323
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to	https://www.qualcomm.com/company/product-	H-QUA-QCS6-031121/2324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2325
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2327
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2328
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2329
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS6-031121/2330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2331
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2332
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCS6-031121/2333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2334
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2335
qcs6125					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-QCS6-031121/2336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2337
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2338
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2340
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2341
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2343
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2344
Buffer Copy without Checking Size of Input	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in	https://www.qualcomm.com/company/product-	H-QUA-QCS6-031121/2345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2346
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2347
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2349
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2350
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2351
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory	https://www.qualcomm.com/compan	H-QUA-QCS6-031121/2352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2353
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2354
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qcs6490					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2356
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2357
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2359
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2360
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2361
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS6-031121/2362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2363
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2364
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2365
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS6-031121/2366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	etins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2367
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2368
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in	https://www.qualcomm.com/company/product-	H-QUA-QCS6-031121/2369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2370
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCS6-031121/2371
qcx315					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QCX3-031121/2372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCX3-031121/2373
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCX3-031121/2374
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information	https://www.qualcomm.com/company/product-	H-QUA-QCX3-031121/2375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCX3-031121/2376
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QCX3-031121/2377
qet4101					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QET4-031121/2378
qrb5165					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QRB5-031121/2379
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QRB5-031121/2380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1967		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QRB5-031121/2381
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QRB5-031121/2382
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-QRB5-031121/2383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QRB5-031121/2384
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QRB5-031121/2385
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in	https://www.qualcomm.com/company/product-	H-QUA-QRB5-031121/2386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	security/bulletins/october-2021-bulletin	
qsm8250					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QSM8-031121/2387
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QSM8-031121/2388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30312**		
qsm8350					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QSM8-031121/2389
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QSM8-031121/2390
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QSM8-031121/2391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QSM8-031121/2392
qsw8573					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QSW8-031121/2393
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QSW8-031121/2394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	etins/octobe r-2021-bulletin	
qualcomm215					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2395
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2396
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1949		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2398
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2399
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2401
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2402
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2403
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30257		
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2405
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2406
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2407
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-QUAL-031121/2408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**		
sa415m					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA41-031121/2409
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA41-031121/2410
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA41-031121/2411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA41-031121/2412
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA41-031121/2413
Improper	20-Oct-21	7.2	Possible out of bound	https://ww	H-QUA-SA41-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/2414
sa515m					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA51-031121/2415
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA51-031121/2416
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while	https://www.qualcomm.com/compan	H-QUA-SA51-031121/2417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA51-031121/2418
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA51-031121/2419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA51-031121/2420
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA51-031121/2421
sa6145p					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1917		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2423
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2424
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2425
Buffer Copy without Checking Size of Input	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in	https://www.qualcomm.com/company/product-	H-QUA-SA61-031121/2426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2427
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2428
Exposure of Resource to Wrong	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to	https://www.qualcomm.com/compan	H-QUA-SA61-031121/2429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2430
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2432
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2433
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2434
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SA61-031121/2435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2436
sa6150p					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2437
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1936**		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2439
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2440
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2441
Out-of-	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check	https://www.qualcomm.	H-QUA-SA61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	com/company/product-security/bulletins/october-2021-bulletin	031121/2442
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2443
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1969		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2445
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2446
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SA61-031121/2447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile **CVE ID : CVE-2021-30305**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2448
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2449
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2451
sa6155					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2452
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2453
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://www.qualcomm.com/compan	H-QUA-SA61-031121/2454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2455
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2456
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to	https://www.qualcomm.com/company/product-	H-QUA-SA61-031121/2457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2458
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2460
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2461
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2462
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA61-031121/2463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	etins/octobe r-2021-bulletin	
Improper Authenticatio n	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-SA61-031121/2464
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-SA61-031121/2465
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-	H-QUA-SA61-031121/2466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	bulletin	
sa6155p					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2467
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2468
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2470
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2471
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2473
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2474
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1968		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2476
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2477
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2479
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2480
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2482
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2483
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA61-031121/2484
sa8145p					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in	https://www.qualcomm.com/compan	H-QUA-SA81-031121/2485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	y/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2486
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2487
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2489
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2490
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2492
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2493
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SA81-031121/2494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2495
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2496
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2498
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2499
sa8150p					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2500
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application	https://www.qualcomm.	H-QUA-SA81-031121/2501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	com/company/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2502
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2503
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://www.qualcomm.com/compan	H-QUA-SA81-031121/2504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2505
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2506
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to	https://www.qualcomm.com/company/product-	H-QUA-SA81-031121/2507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2508
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2510
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2511
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2512
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA81-031121/2513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	etins/octobe r-2021-bulletin	
Improper Authenticatio n	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-SA81-031121/2514
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-SA81-031121/2515
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-	H-QUA-SA81-031121/2516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	bulletin	
sa8155					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2517
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2518
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1936		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2520
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2521
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2522
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of	https://www.qualcomm.com/compan	H-QUA-SA81-031121/2523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	y/product-security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2524
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1969		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2526
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2527
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SA81-031121/2528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	r-2021-bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2529
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2530
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2532
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2533
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2534
sa8155p					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2535
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2536
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2537
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in	https://www.qualcomm.com/company/product-	H-QUA-SA81-031121/2538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2539
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2540
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2542
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2543
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption	https://www.qualcomm.com/company/product-	H-QUA-SA81-031121/2544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2545
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2547
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2548
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2549
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in	https://www.qualcomm.com/company/product-	H-QUA-SA81-031121/2550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	security/bulletins/october-2021-bulletin	
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2551
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2552
sa8195p					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SA81-031121/2553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	bulletin	
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2554
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2555
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1936**		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2557
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2558
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2559
Out-of-	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check	https://www.qualcomm.	H-QUA-SA81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	com/company/product-security/bulletins/october-2021-bulletin	031121/2560
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2561
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1969		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2563
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2564
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SA81-031121/2565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile **CVE ID : CVE-2021-30305**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2566
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2567
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2569
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SA81-031121/2570
sc8180x\\+sdx55					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SC81-031121/2571
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SC81-031121/2572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SC81-031121/2573
sc8280xp					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SC82-031121/2574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SC82-031121/2575
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SC82-031121/2576
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-SC82-031121/2577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	y/product-security/bulletins/october-2021-bulletin	
sd205					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD20-031121/2578
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD20-031121/2579
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD20-031121/2580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD20-031121/2581
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD20-031121/2582
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD20-031121/2583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD20-031121/2584
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD20-031121/2585
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD20-031121/2586
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD20-031121/2587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30297**		
sd210					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD21-031121/2588
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD21-031121/2589
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD21-031121/2590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1967		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD21-031121/2591
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD21-031121/2592
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD21-031121/2593
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD21-031121/2594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD21-031121/2595
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD21-031121/2596
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD21-031121/2597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30292**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD21-031121/2598
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD21-031121/2599
sd429					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD42-031121/2600
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null	https://www.qualcomm.	H-QUA-SD42-031121/2601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	com/company/product-security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD42-031121/2602
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD42-031121/2603
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD42-031121/2604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD42-031121/2605
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD42-031121/2606
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD42-031121/2607
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in	https://www.qualcomm.com/company/product-	H-QUA-SD42-031121/2608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD42-031121/2609
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD42-031121/2610
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD42-031121/2611
Buffer Copy without Checking Size of Input	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR	https://www.qualcomm.com/company/product-	H-QUA-SD42-031121/2612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	security/bulletins/october-2021-bulletin	
sd439					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD43-031121/2613
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD43-031121/2614
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD43-031121/2615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1949		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD43-031121/2616
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD43-031121/2617
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD43-031121/2618
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-SD43-031121/2619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD43-031121/2620
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD43-031121/2621
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD43-031121/2622
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-SD43-031121/2623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD43-031121/2624
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD43-031121/2625
sd450					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD45-031121/2626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD45-031121/2627
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD45-031121/2628
sd460					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-031121/2629
NULL Pointer	20-Oct-21	7.2	Null pointer dereference can	https://ww	H-QUA-SD46-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/2630
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-031121/2631
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-031121/2632
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD46-031121/2633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-031121/2634
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-031121/2635
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD46-031121/2636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-031121/2637
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-031121/2638
Buffer Copy	20-Oct-21	7.2	Possible buffer overflow due	https://ww	H-QUA-SD46-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	031121/2639
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-031121/2640
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-031121/2641
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-041121/2642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-041121/2643
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-041121/2644
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-041121/2645
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of	https://www.qualcomm.	H-QUA-SD46-041121/2646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	com/company/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-041121/2647
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-041121/2648
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD46-041121/2649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
sd480					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2650
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2651
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2653
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2654
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2656
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2657
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2658
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before	https://www.qualcomm.com/compan	H-QUA-SD48-041121/2659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2660
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2661
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2663
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2664
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD48-041121/2665
Improper Restriction of Operations within the Bounds of a	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD48-041121/2666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	etins/october-2021-bulletin	
sd632					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD63-041121/2667
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD63-041121/2668
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD63-041121/2669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD63-041121/2670
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD63-041121/2671
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD63-041121/2672
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD63-041121/2673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD63-041121/2674
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD63-041121/2675
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD63-041121/2676
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD63-041121/2677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD63-041121/2678
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD63-041121/2679
sd660					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2681
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2682
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD66-041121/2683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2684
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2685
sd662					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2686
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2687
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2688
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can	https://ww	H-QUA-SD66-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/2689
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2690
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2691
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD66-041121/2692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2693
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2695
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2696
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2697
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD66-041121/2698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2699
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2700
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30288		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2702
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2703
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2704
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD66-041121/2705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile **CVE ID : CVE-2021-30306**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2706
sd665					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2707
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2709
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2710
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2711
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery	https://www.qualcomm.com/company/product-	H-QUA-SD66-041121/2712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2713
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2715
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2718
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2719
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2720
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD66-041121/2721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2722
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2723
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30291**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2725
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2726
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD66-041121/2727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd670					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2728
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2729
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
sd675					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2731
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2732
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2734
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2735
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2737
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2738
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2740
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2741
Buffer Copy	20-Oct-21	7.2	Possible buffer overflow due	https://ww	H-QUA-SD67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/2742
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2743
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2744
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT **CVE ID : CVE-2021-30256**		
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2746
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2747
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2749
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2750
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2751
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2753
sd678					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2754
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2756
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2757
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2759
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2760
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2762
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2763
Buffer Copy without	20-Oct-21	7.2	Possible buffer overflow due to improper handling of	https://www.qualcomm.	H-QUA-SD67-041121/2764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	com/company/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2765
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2766
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30256		
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2768
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2769
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2770
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of	https://www.qualcomm.	H-QUA-SD67-041121/2771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2772
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2773
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD67-041121/2775
sd690_5g					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2776
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2777
Integer	20-Oct-21	7.2	Possible integer overflow	https://ww	H-QUA-SD69-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/2778
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2779
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2780
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD69-041121/2781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2782
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2784
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2785
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2786
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD69-041121/2787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	etins/octobe r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2788
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2789
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2791
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2792
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2793
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD69-041121/2794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	r-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2795
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD69-041121/2796
sd710					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD71-041121/2797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD71-041121/2798
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD71-041121/2799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd712					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD71-041121/2800
sd720g					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2801
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2803
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2804
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2805
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD72-041121/2806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	etins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2807
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2808
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	H-QUA-SD72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/2809
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2810
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1983**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2812
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2813
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2814
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD72-041121/2815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2816
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2817
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30291		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2819
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2820
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD72-041121/2821
Improper	20-Oct-21	7.2	Possible out of bound	https://ww	H-QUA-SD72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/2822
sd730					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2823
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2824
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided	https://www.qualcomm.com/compan	H-QUA-SD73-041121/2825

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	y/product-security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2826
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2827
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2829
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2830
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1985		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2832
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2833
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2834
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2836
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2837
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD73-041121/2839
sd750g					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2840
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2841
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while	https://www.qualcomm.com/compan	H-QUA-SD75-041121/2842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2843
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2844
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD75-041121/2845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2846
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2848
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2849
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2850
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD75-041121/2851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2852
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2853
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30288		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2855
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2856
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2857
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD75-041121/2858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile **CVE ID : CVE-2021-30306**	bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2859
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD75-041121/2860
sd765					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD76-041121/2861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1917**	bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2862
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2863
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2864
Buffer Copy without Checking Size	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination	https://www.qualcomm.com/compan	H-QUA-SD76-041121/2865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2866
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2868
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2869
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2870
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	H-QUA-SD76-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/2871
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2872
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2873
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2875
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2876
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2877
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	H-QUA-SD76-041121/2878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2879
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2880
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
sd765g					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2882
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2883
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1949		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2885
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2886
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2888
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2889
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2891
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2892
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2893
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD76-041121/2894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2895
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2896
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30291**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2898
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2899
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2900
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD76-041121/2901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2902
sd768g					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2903
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD76-041121/2904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2905
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2906
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2908
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2909
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2911
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2912
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2914
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2915
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2916
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2918
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2919
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2921
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2922
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD76-041121/2923
sd778g					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2924
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2925
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2926
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD77-041121/2927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2928
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2929
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD77-041121/2930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2931
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2932
Buffer Copy without Checking Size	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing	https://www.qualcomm.com/compan	H-QUA-SD77-041121/2933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2934
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2935
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2936
Out-of-	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation	https://www.qualcomm.	H-QUA-SD77-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	com/company/product-security/bulletins/october-2021-bulletin	041121/2937
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2938
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2939
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-SD77-041121/2940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2941
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2942
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD77-041121/2943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30305	bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2944
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2945
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD77-041121/2946
sd780g					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2947
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2948
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2949
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD78-041121/2950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2951
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2952
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE	https://www.qualcomm.com/compan	H-QUA-SD78-041121/2953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2954
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2955
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-SD78-041121/2956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2957
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2958
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2959
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in	https://www.qualcomm.com/company/product-	H-QUA-SD78-041121/2960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2961
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2962
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD78-041121/2963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2964
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2965
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2966
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	H-QUA-SD78-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	041121/2967
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD78-041121/2968
sd7c					
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD7C-041121/2969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1932**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD7C-041121/2970
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD7C-041121/2971
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD7C-041121/2972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
sd820					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD82-041121/2973
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD82-041121/2974
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD82-041121/2975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	etins/octobe r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD82-041121/2976
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD82-041121/2977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD82-041121/2978
sd821					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD82-041121/2979
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD82-041121/2980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
sd835					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD83-041121/2981
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD83-041121/2982
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD83-041121/2983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
sd845					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD84-041121/2984
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD84-041121/2985
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD84-041121/2986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD84-041121/2987
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD84-041121/2988
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of	https://www.qualcomm.	H-QUA-SD84-041121/2989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD84-041121/2990
sd850					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/2991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/2992
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/2993
sd855					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace	https://www.qualcomm.com/compan	H-QUA-SD85-041121/2994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	y/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/2995
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/2996
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SD85-041121/2997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/2998
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/2999
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-1966**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3001
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3002
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3004
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3005
Buffer Copy	20-Oct-21	7.2	Possible buffer overflow due	https://ww	H-QUA-SD85-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/3006
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3007
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3008
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT **CVE ID : CVE-2021-30256**		
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3010
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3011
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3013
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3014
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3015
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD85-041121/3016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
sd865_5g					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3017
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3018
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1936**		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3020
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3021
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3022
Out-of-	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check	https://www.qualcomm.	H-QUA-SD86-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	com/company/product-security/bulletins/october-2021-bulletin	041121/3023
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3024
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3026
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3027
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3028
Out-of-	20-Oct-21	7.2	Possible stack overflow due to improper validation of	https://www.qualcomm.	H-QUA-SD86-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	com/company/product-security/bulletins/october-2021-bulletin	041121/3029
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3030
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3031
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3033
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3034
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3035
Improper Authenticatio	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user	https://www.qualcomm.com/compan	H-QUA-SD86-041121/3036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3037
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD86-041121/3038
sd870					
Integer	20-Oct-21	7.2	Possible integer overflow	https://ww	H-QUA-SD87-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/3039
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3040
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3041
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3043
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3044
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3046
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3047
Buffer Copy without Checking Size of Input	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in	https://www.qualcomm.com/company/product-	H-QUA-SD87-041121/3048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3049
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3050
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3052
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3053
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3054
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory	https://www.qualcomm.com/compan	H-QUA-SD87-041121/3055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3056
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3057
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3059
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD87-041121/3060
sd888					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1917		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3062
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3063
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3065
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3066
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3067
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	H-QUA-SD88-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/3068
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3069
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3070
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3072
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3073
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3074
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	H-QUA-SD88-041121/3075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3076
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3077
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD88-041121/3078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3079
sd888_5g					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3080
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SD88-041121/3081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	security/bulletins/october-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3082
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3083
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3085
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3086
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3088
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3089
Buffer Copy without Checking Size of Input	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in	https://www.qualcomm.com/company/product-	H-QUA-SD88-041121/3090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3091
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3092
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3093
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR	https://www.qualcomm.com/compan	H-QUA-SD88-041121/3094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3095
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3096
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD88-041121/3097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	etins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3098
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3099
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3101
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3102
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD88-041121/3103
sda429w					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory	https://www.qualcomm.	H-QUA-SDA4-041121/3104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	com/company/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDA4-041121/3105
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDA4-041121/3106
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDA4-041121/3107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDA4-041121/3108
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDA4-041121/3109
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SDA4-041121/3110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDA4-041121/3111
sdm429w					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM4-041121/3112
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SDM4-041121/3113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM4-041121/3114
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM4-041121/3115
sdm630					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM6-041121/3116
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	SDM6-041121/3117
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM6-041121/3118
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM6-041121/3119
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SDM6-041121/3120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM6-041121/3121
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM6-041121/3122
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SDM6-041121/3123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM6-041121/3124
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM6-041121/3125
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM6-041121/3126
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SDM6-041121/3127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM6-041121/3128
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM6-041121/3129
sdm830					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM8-041121/3130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM8-041121/3131
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM8-041121/3132
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDM8-041121/3133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
sdw2500					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDW2-041121/3134
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDW2-041121/3135
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDW2-041121/3136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
sdx12					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX1-041121/3137
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX1-041121/3138
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX1-041121/3139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX1-041121/3140
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX1-041121/3141
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX1-041121/3142
Improper Restriction of Operations within the Bounds of a Memory	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SDX1-041121/3143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	r-2021-bulletin	
sdx20					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3144
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3145
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3147
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3148
sdx20m					
Integer	20-Oct-21	7.2	Possible integer overflow	https://ww	H-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/3149
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3150
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3152
sdx24					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3153
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3155
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX2-041121/3156
Improper Input	20-Oct-21	5	Possible buffer overflow due to Improper validation of	https://www.qualcomm.	H-QUA-SDX2-041121/3157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	com/company/product-security/bulletins/october-2021-bulletin	
sdx50m					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3158
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3159
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null	https://www.qualcomm.	H-QUA-SDX5-041121/3160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	com/company/product-security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3161
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3162
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SDX5-041121/3163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3164
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3165
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1985**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3167
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3168
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3169
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SDX5-041121/3170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3171
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3172
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30297		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3174
sdx55					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3175
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1917		
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3177
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3178
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3180
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3181
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3182
Exposure of	20-Oct-21	2.1	Improper validation of	https://ww	H-QUA-SDX5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/3183
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3184
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3186
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3187
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1984**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3189
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3190
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3191
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SDX5-041121/3192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30258**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3193
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3194
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3196
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3197
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3199
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3200
sdx55m					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3202
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3203
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3204
Integer Overflow or	20-Oct-21	7.2	Possible integer overflow due to improper check of	https://www.qualcomm.	H-QUA-SDX5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	com/company/product-security/bulletins/october-2021-bulletin	041121/3205
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3206
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3207
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SDX5-041121/3208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	r-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3209
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3210
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation	https://www.qualcomm.	H-QUA-SDX5-041121/3211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3212
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1983		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3214
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3215
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3216
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SDX5-041121/3217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3218
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3219
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3221
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3222
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3223
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length	https://www.qualcomm.com/compan	H-QUA-SDX5-041121/3224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	y/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3225
sdx57m					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDX5-041121/3226
sdxr1					
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can	https://ww	H-QUA-SDXR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/3227
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3228
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3229
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SDXR-041121/3230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3231
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3232
Buffer Copy without	20-Oct-21	7.2	Possible buffer overflow due to improper validation of	https://www.qualcomm.	H-QUA-SDXR-041121/3233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3234
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3235
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3237
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3238
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3239
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of	https://www.qualcomm.	H-QUA-SDXR-041121/3240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	com/company/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3241
sdxr2_5g					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3242
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SDXR-041121/3243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	r-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3244
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3245
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3247
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3248
Buffer Copy without Checking Size	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while	https://www.qualcomm.com/compan	H-QUA-SDXR-041121/3249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3250
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3251
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3253
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3254
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3255
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory	https://www.qualcomm.com/compan	H-QUA-SDXR-041121/3256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3257
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3258
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SDXR-041121/3260
sd_455					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_4-041121/3261
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_4-041121/3262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_4-041121/3263
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_4-041121/3264
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_4-041121/3265
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR	https://www.qualcomm.com/compan	H-QUA-SD_4-041121/3266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_4-041121/3267
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_4-041121/3268
sd_636					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3269
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can	https://ww	H-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/3270
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3271
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3272
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SD_6-041121/3273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3274
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3275
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD_6-041121/3276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3277
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3278
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3279
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SD_6-041121/3280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3281
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3282
sd_675					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3283
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP	https://www.qualcomm.com/company/product-	H-QUA-SD_6-041121/3284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3285
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3286
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD_6-041121/3287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3288
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3289
Exposure of Resource to Wrong	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to	https://www.qualcomm.com/compan	H-QUA-SD_6-041121/3290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3291
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3293
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3294
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3295
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR	https://www.qualcomm.com/company/product-	H-QUA-SD_6-041121/3296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3297
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3298
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3300
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3301
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3302
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD_6-041121/3303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	etins/october-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_6-041121/3304
sd_8c					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3305
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause	https://www.qualcomm.com/compan	H-QUA-SD_8-041121/3306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3307
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3308
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of	https://www.qualcomm.com/compan	H-QUA-SD_8-041121/3309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	y/product-security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3310
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1969		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3312
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3313
sd_8cx					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD_8-041121/3314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	etins/october-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3315
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3316
Buffer Copy without Checking Size	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination	https://www.qualcomm.com/compan	H-QUA-SD_8-041121/3317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3318
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3319
Exposure of Resource to	20-Oct-21	2.1	Improper validation of kernel buffer address while	https://www.qualcomm.	H-QUA-SD_8-041121/3320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3321
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SD_8-041121/3323
sm4125					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3324
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM41-041121/3325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	etins/octobe r-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-SM41-041121/3326
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-SM41-041121/3327
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-SM41-041121/3328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3329
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3330
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3332
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3333
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1985		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3335
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3336
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3337
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3339
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3340
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM41-041121/3342
sm6250					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3343
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3345
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3346
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3347
Out-of-	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check	https://www.qualcomm.	H-QUA-SM62-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	com/company/product-security/bulletins/october-2021-bulletin	041121/3348
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3349
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1969		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3351
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3352
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SM62-041121/3353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3354
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3355
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3356
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP	https://www.qualcomm.com/compan	H-QUA-SM62-041121/3357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3358
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3359
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SM62-041121/3360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3361
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3362
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3364
sm6250p					
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3365
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1936		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3367
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3368
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3370
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3371
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3372
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM62-041121/3373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3374
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3375
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-SM62-041121/3376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3377
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM62-041121/3378
sm7250					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1917		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3380
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3381
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3382
Buffer Copy without Checking Size of Input	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in	https://www.qualcomm.com/company/product-	H-QUA-SM72-041121/3383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3384
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3385
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	H-QUA-SM72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	041121/3386
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3387
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3388
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length	https://www.qualcomm.	H-QUA-SM72-041121/3389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3390
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3391
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3392
Out-of-	20-Oct-21	7.2	Possible stack overflow due to improper length check of	https://www.qualcomm.	H-QUA-SM72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	com/company/product-security/bulletins/october-2021-bulletin	041121/3393
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3394
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3395
Buffer Copy without Checking Size of Input	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR	https://www.qualcomm.com/company/product-	H-QUA-SM72-041121/3396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3397
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3398
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM72-041121/3399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
sm7325					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3400
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3401
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1936		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3403
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3404
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1967		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3406
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3407
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SM73-041121/3408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3409
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3410
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3411
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP	https://www.qualcomm.com/compan	H-QUA-SM73-041121/3412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3413
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3414
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-SM73-041121/3415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3416
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3417
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30302		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3419
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3420
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-SM73-041121/3421
Improper Restriction of Operations within the Bounds of a	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM73-041121/3422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	etins/octobe r-2021-bulletin	
wcd9306					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3423
wcd9326					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3424
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCD9-041121/3425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3426
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3428
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3429
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30310		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3431
wcd9330					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3432
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3434
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3435
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-041121/3436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	etins/october-2021-bulletin	
wcd9335					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3437
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3438
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCD9-041121/3439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3440
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3441
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while	https://www.qualcomm.com/compan	H-QUA-WCD9-041121/3442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3443
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3445
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3446
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3447
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to	https://www.qualcomm.com/compan	H-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	y/product-security/bulletins/october-2021-bulletin	041121/3448
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3449
wcd9340					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3450
Incorrect	20-Oct-21	7.2	Improper access control in	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCD9-041121/3451
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3452
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3453
Out-of-	20-Oct-21	4.6	Possible stack buffer	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCD9-041121/3454
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3455
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3457
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3458
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-041121/3459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	etins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3460
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30310		
wcd9341					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3462
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3463
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3465
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3466
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3468
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3469
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-WCD9-041121/3470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3471
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3473
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3474
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3475
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-041121/3476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	etins/october-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3477
wcd9360					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3478
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause	https://www.qualcomm.com/compan	H-QUA-WCD9-041121/3479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3480
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3482
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3483
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**		
wcd9370					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3485
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3486
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3488
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3489
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3490
Buffer Copy without	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of	https://www.qualcomm.	H-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	com/company/product-security/bulletins/october-2021-bulletin	041121/3491
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3492
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3493
Exposure of	20-Oct-21	2.1	Improper validation of	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCD9-041121/3494
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3495
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3497
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3498
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3499
Out-of-	20-Oct-21	7.2	Possible stack overflow due to improper validation of	https://www.qualcomm.	H-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	com/company/product-security/bulletins/october-2021-bulletin	041121/3500
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3501
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3502
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3504
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3505
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3506
Improper Authenticatio	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user	https://www.qualcomm.com/compan	H-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	y/product-security/bulletins/october-2021-bulletin	041121/3507
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3508
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3509
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3511
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3512
wcd9371					
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3514
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3515
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3517
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3518
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1984**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3520
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3521
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wcd9375					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3523
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3524
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3526
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3527
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3528
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-041121/3529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3530
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3531
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to	https://www.qualcomm.com/company/product-	H-QUA-WCD9-041121/3532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3533
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3535
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3536
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3537
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-041121/3538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	etins/octobe r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3539
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3540
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3542
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3543
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3544
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCD9-041121/3545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	r-2021-bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3546
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3547
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3549
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3550
wcd9380					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3552
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3553
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3554
Integer Overflow or	20-Oct-21	7.2	Possible integer overflow due to improper check of	https://www.qualcomm.	H-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	com/company/product-security/bulletins/october-2021-bulletin	041121/3555
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3556
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3557
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCD9-041121/3558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	r-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3559
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3560
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation	https://www.qualcomm.	H-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	com/company/product-security/bulletins/october-2021-bulletin	041121/3561
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3562
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1983		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3564
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3565
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3566
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCD9-041121/3567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3568
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3569
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3571
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3572
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3573
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-WCD9-041121/3574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	y/product-security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3575
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3576
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3577
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	H-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	041121/3578
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3579
wcd9385					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3581
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3582
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3583
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in	https://www.qualcomm.com/company/product-	H-QUA-WCD9-041121/3584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3585
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3586
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3588
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3590
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3591
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3592
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCD9-041121/3593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3594
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3595
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3597
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3598
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3599
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3601
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3602
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3603
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-041121/3604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	etins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3605
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCD9-041121/3606
wcn3610					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in	https://www.qualcomm.com/compan	H-QUA-WCN3-041121/3607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	y/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3608
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3609
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3611
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3612
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3614
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3615
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN3-041121/3616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3617
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3618
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3620
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3621
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3622
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN3-041121/3623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3624
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3625
wcn3615					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-WCN3-041121/3626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3627
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3628
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3630
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3631
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3633
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3634
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3636
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3637
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3638
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3640
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3641
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3643
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3644
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3645
wcn3620					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3646
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3647
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3648
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-041121/3649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	etins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3650
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3651
Out-of-	20-Oct-21	7.2	Possible buffer overflow due	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCN3-041121/3652
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3653
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3654
wcn3660					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null	https://www.qualcomm.	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	com/company/product-security/bulletins/october-2021-bulletin	041121/3655
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3656
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3657
wcn3660b					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN3-041121/3658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	r-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3659
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3660
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3661
Out-of-	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check	https://www.qualcomm.	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	com/company/product-security/bulletins/october-2021-bulletin	041121/3662
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3663
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1969		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3665
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3666
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3668
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3669
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3670
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3672
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3673
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3674
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	041121/3675
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3676
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3677
Improper	20-Oct-21	7.2	Possible out of bound	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCN3-041121/3678
wcn3680					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3679
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3680
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN3-041121/3681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3682
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3683
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN3-041121/3684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3685
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3686
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3687
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN3-041121/3688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3689
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3690
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3691
wcn3680b					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory	https://www.qualcomm.	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	com/company/product-security/bulletins/october-2021-bulletin	041121/3692
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3693
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3694
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3696
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3697
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN3-041121/3698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3699
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3700
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN3-041121/3701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3702
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3703
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3704
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN3-041121/3705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3706
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3707
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30297**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3709
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3710
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3712
wcn3910					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3713
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3714
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause	https://www.qualcomm.com/compan	H-QUA-WCN3-041121/3715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	y/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3716
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3717
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-WCN3-041121/3718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3719
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3721
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3722
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3723
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN3-041121/3724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3725
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3726
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30288		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3728
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3729
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3730
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN3-041121/3731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3732
wcn3950					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3733
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in	https://www.qualcomm.com/compan	H-QUA-WCN3-041121/3734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	y/product-security/bulletins/october-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3735
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3736
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN3-041121/3737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3738
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3739
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3741
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3742
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN3-041121/3743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3744
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3745
Buffer Copy without Checking Size	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing	https://www.qualcomm.com/compan	H-QUA-WCN3-041121/3746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3747
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3748
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3749
Out-of-	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation	https://www.qualcomm.	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	com/company/product-security/bulletins/october-2021-bulletin	041121/3750
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3751
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3752
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-WCN3-041121/3753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3754
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3755
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3757
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3758
wcn3980					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1913**		
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3760
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3761
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-1966**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3763
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3764
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3766
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3767
Out-of-	20-Oct-21	7.2	Possible stack overflow due	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCN3-041121/3768
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3769
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**		
wcn3988					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3771
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3772
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3774
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3775
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3776
Buffer Copy without	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of	https://www.qualcomm.	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	com/company/product-security/bulletins/october-2021-bulletin	041121/3777
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3778
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3779
Exposure of	20-Oct-21	2.1	Improper validation of	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCN3-041121/3780
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3781
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3783
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3784
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3785
Out-of-	20-Oct-21	7.2	Possible stack overflow due to improper validation of	https://www.qualcomm.	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	com/company/product-security/bulletins/october-2021-bulletin	041121/3786
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3787
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3788
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3790
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3791
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3792
Improper Input	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is	https://www.qualcomm.com/compan	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	y/product-security/bulletins/october-2021-bulletin	041121/3793
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3794
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3795
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3797
wcn3990					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3798
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3800
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3801
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN3-041121/3802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3803
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3805
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3806
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN3-041121/3807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	bulletin	
wcn3991					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3808
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3809
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3811
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3812
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3814
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3815
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1968		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3817
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3818
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3820
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3821
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1985		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3823
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3824
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3825
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3827
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3828
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3830
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3831
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3832
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3834
wcn3998					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3835
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN3-041121/3836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1917**	bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3837
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3838
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1949		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3840
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3841
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3843
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3844
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3846
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3847
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3849
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3850
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3851
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN3-041121/3852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3853
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3854
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30292		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3856
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3857
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3858
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll	https://www.qualcomm.com/compan	H-QUA-WCN3-041121/3859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	y/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3860
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3861
wcn3999					
Integer	20-Oct-21	7.2	Possible integer overflow	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCN3-041121/3862
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3863
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1949		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3865
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3866
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3868
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3869
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN3-041121/3870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3871
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN3-041121/3872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30312**		
wcn6740					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3873
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3874
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3875
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while	https://www.qualcomm.com/compan	H-QUA-WCN6-041121/3876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3877
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3879
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3880
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3882
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3883
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3884
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3886
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3887
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3888
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	H-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	041121/3889
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3890
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3891
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN6-041121/3892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile **CVE ID : CVE-2021-30306**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3893
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3894
wcn6750					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3896
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3897
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3898
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-WCN6-041121/3899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3900
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3902
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3903
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3904
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCN6-041121/3905
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3906
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3907
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3909
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3910
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3911
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	H-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	041121/3912
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3913
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3914
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WCN6-041121/3915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile **CVE ID : CVE-2021-30306**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3916
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3917
wcn6850					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3919
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3920
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3922
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3923
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3924
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery	https://www.qualcomm.com/company/product-	H-QUA-WCN6-041121/3925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3926
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3928
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3929
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3930
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR	https://www.qualcomm.com/company/product-	H-QUA-WCN6-041121/3931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3932
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3933
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3935
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3936
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3937
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN6-041121/3938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3939
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3940
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3941
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	H-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	041121/3942
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3943
wcn6851					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3945
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3946
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3947
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3949
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3950
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3952
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3953
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN6-041121/3954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	etins/octobe r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-WCN6-041121/3955
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-WCN6-041121/3956
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-WCN6-041121/3957
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	H-QUA-WCN6-041121/3958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3959
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3960
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN6-041121/3961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3962
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3963
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30304		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3965
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3966
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3967
Improper Restriction of Operations within the Bounds of a	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN6-041121/3968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	etins/octobe r-2021-bulletin	
wcn6855					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-WCN6-041121/3969
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-WCN6-041121/3970
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	H-QUA-WCN6-041121/3971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1936		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3972
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3973
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1967		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3975
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3976
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN6-041121/3977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3978
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3979
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3980
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP	https://www.qualcomm.com/compan	H-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	y/product-security/bulletins/october-2021-bulletin	041121/3981
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3982
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3983
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WCN6-041121/3984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3985
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3986
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30302		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3988
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3989
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3990
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3992
wcn6856					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3993
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1917		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3995
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3996
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3997
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery	https://www.qualcomm.com/company/product-	H-QUA-WCN6-041121/3998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/3999
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4001
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4002
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4003
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR	https://www.qualcomm.com/company/product-	H-QUA-WCN6-041121/4004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4005
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4006
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4008
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4009
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4010
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN6-041121/4011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4012
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4013
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4014
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	H-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	041121/4015
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WCN6-041121/4016
whs9410					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WHS9-041121/4017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WHS9-041121/4018
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WHS9-041121/4019
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WHS9-041121/4020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
wsa8810					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4021
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4022
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-WSA8-041121/4023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4024
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4025
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information	https://www.qualcomm.com/company/product-security/bull	H-QUA-WSA8-041121/4026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	etins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4027
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4029
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4030
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WSA8-041121/4031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4032
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4033
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4035
wsa8815					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4036
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WSA8-041121/4037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4038
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4039
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WSA8-041121/4040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4041
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4042
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while	https://www.qualcomm.com/compan	H-QUA-WSA8-041121/4043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4044
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4046
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4047
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4049
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4050
wsa8830					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WSA8-041121/4051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	bulletin	
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4052
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4053
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4054
Out-of-	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of	https://www.qualcomm.	H-QUA-WSA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	com/company/product-security/bulletins/october-2021-bulletin	041121/4055
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4056
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4057
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while	https://www.qualcomm.com/compan	H-QUA-WSA8-041121/4058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4059
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1983		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4061
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4062
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4063
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	H-QUA-WSA8-041121/4064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4065
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4066
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4068
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4069
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4070
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-WSA8-041121/4071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	y/product-security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4072
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4073
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4074
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	H-QUA-WSA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	041121/4075
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4076
wsa8835					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4078
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4079
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4080
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4082
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4083
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4085
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4086
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WSA8-041121/4087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4088
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4089
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4090
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-WSA8-041121/4091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4092
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4093
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	H-QUA-WSA8-041121/4094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4095
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4096
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30304		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4098
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4099
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4100
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	H-QUA-WSA8-041121/4102
skyworth					
penguin_aurora_box					
Incorrect Authorization	26-Oct-21	6.4	Penguin Aurora TV Box 41502 is a high-end network HD set-top box produced by Tencent Video and Skyworth Digital. An unauthorized access vulnerability exists in the Penguin Aurora Box. An attacker can use the vulnerability to gain unauthorized access to a specific link to remotely control the TV. **CVE ID : CVE-2021-41873**	N/A	H-SKY-PENG-041121/4103
Trane					
tracer_sc					
Improper Input	27-Oct-21	6.5	The affected controllers do not properly sanitize the	https://us-cert.cisa.gov/	H-TRA-TRAC-041121/4104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software. **CVE ID : CVE-2021-38450**	ics/advisories/icsa-21-266-02	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-21	4.3	The affected product's web application does not properly neutralize the input during webpage generation, which could allow an attacker to inject code in the input forms. **CVE ID : CVE-2021-42534**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-02	H-TRA-TRAC-041121/4105
tracer_sc\\+					
Improper Input Validation	27-Oct-21	6.5	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software. **CVE ID : CVE-2021-38450**	https://us-cert.cisa.gov/ics/advisories/icsa-21-266-02	H-TRA-TRAC-041121/4106
ZTE					
mf971r					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Oct-21	4.3	ZTE MF971R product has a CRLF injection vulnerability. An attacker could exploit the vulnerability to modify the HTTP response header information through a specially crafted HTTP request. **CVE ID : CVE-2021-21743**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	H-ZTE-MF97-041121/4107
N/A	20-Oct-21	5	ZTE MF971R product has a configuration file control vulnerability. An attacker could use this vulnerability	https://support.zte.com.cn/support/news/Loophol	H-ZTE-MF97-041121/4108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to modify the configuration parameters of the device, causing some security functions of the device to be disabled. **CVE ID : CVE-2021-21744**	eInfoDetail.aspx?newsId=1019764	
Improper Authentication	20-Oct-21	4.3	ZTE MF971R product has a Referer authentication bypass vulnerability. Without CSRF verification, an attackercould use this vulnerability to perform illegal authorization operations by sending a request to the user to click. **CVE ID : CVE-2021-21745**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	H-ZTE-MF97-041121/4109
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-21	4.3	ZTE MF971R product has reflective XSS vulnerability. An attacker could use the vulnerability to obtain cookie information. **CVE ID : CVE-2021-21746**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	H-ZTE-MF97-041121/4110
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-21	4.3	ZTE MF971R product has reflective XSS vulnerability. An attacker could use the vulnerability to obtain cookie information. **CVE ID : CVE-2021-21747**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	H-ZTE-MF97-041121/4111
Out-of-bounds Write	20-Oct-21	7.5	ZTE MF971R product has two stack-based buffer overflow vulnerabilities. An attacker could exploit the vulnerabilities to execute arbitrary code. **CVE ID : CVE-2021-21748**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	H-ZTE-MF97-041121/4112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.5	ZTE MF971R product has two stack-based buffer overflow vulnerabilities. An attacker could exploit the vulnerabilities to execute arbitrary code. **CVE ID : CVE-2021-21749**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	H-ZTE-MF97-041121/4113
Operating System					
Apple					
ipados					
Missing Authorization	19-Oct-21	2.9	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8, tvOS 15. An attacker in physical proximity may be able to force a user onto a malicious Wi-Fi network during device setup. **CVE ID : CVE-2021-30810**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212814	O-APP-IPAD-051121/4114
N/A	19-Oct-21	2.1	This issue was addressed with improved checks. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8. A local attacker may be able to read sensitive information. **CVE ID : CVE-2021-30811**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212814	O-APP-IPAD-051121/4115
Exposure of Resource to Wrong	19-Oct-21	2.1	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved	https://support.apple.com/en-us/HT21281	O-APP-IPAD-051121/4116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			state management. This issue is fixed in iOS 15 and iPadOS 15. A local attacker may be able to view contacts from the lock screen. **CVE ID : CVE-2021-30815**	4	
Out-of-bounds Read	19-Oct-21	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 15 and iPadOS 15. Processing a maliciously crafted USD file may disclose memory contents. **CVE ID : CVE-2021-30819**	https://support.apple.com/en-us/HT212814	O-APP-IPAD-051121/4117
N/A	19-Oct-21	7.5	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.8 and iPadOS 14.8. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-30820**	https://support.apple.com/en-us/HT212807	O-APP-IPAD-051121/4118
N/A	19-Oct-21	4.6	This issue was addressed with improved checks. This issue is fixed in iOS 15 and iPadOS 15. A local attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-30825**	https://support.apple.com/en-us/HT212814	O-APP-IPAD-051121/4119
N/A	19-Oct-21	5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15 and iPadOS 15. In certain situations, the baseband would fail to enable integrity and	https://support.apple.com/en-us/HT212814	O-APP-IPAD-051121/4120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ciphering protection. **CVE ID : CVE-2021-30826**		
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in Security Update 2021-005 Catalina, iTunes 12.12 for Windows, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30835**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	O-APP-IPAD-051121/4121
N/A	19-Oct-21	9.3	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8, tvOS 15. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-30837**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-	O-APP-IPAD-051121/4122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212814	
N/A	19-Oct-21	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 15 and iPadOS 15. A malicious application may be able to execute arbitrary code with system privileges on devices with an Apple Neural Engine. **CVE ID : CVE-2021-30838**	https://support.apple.com/en-us/HT212814	O-APP-IPAD-051121/4123
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30841**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-	O-APP-IPAD-051121/4124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30842**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	O-APP-IPAD-051121/4125
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-	O-APP-IPAD-051121/4126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30843**	us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
Out-of-bounds Write	19-Oct-21	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-30846**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT21281	O-APP-IPAD-051121/4127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				6, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in watchOS 8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30847**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	O-APP-IPAD-051121/4128
Out-of-bounds Write	19-Oct-21	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 14.8	https://support.apple.com/en-us/HT21280	O-APP-IPAD-051121/4129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 14.8, Safari 15, iOS 15 and iPadOS 15. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2021-30848**	7, https://support.apple.com/en-us/HT212816, https://support.apple.com/en-us/HT212814	
Out-of-bounds Write	19-Oct-21	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, watchOS 8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-30849**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212816, https://support.apple.com/en-us/HT21281	O-APP-IPAD-051121/4130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4	
ipad_os					
N/A	19-Oct-21	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.5.1, iOS 14.7.1 and iPadOS 14.7.1, watchOS 7.6.1. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2021-30807**	https://support.apple.com/en-us/HT212713, https://support.apple.com/en-us/HT212622, https://support.apple.com/en-us/HT212623	O-APP-IPAD-051121/4131
iphone_os					
N/A	19-Oct-21	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.5.1, iOS 14.7.1 and iPadOS 14.7.1, watchOS 7.6.1. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2021-30807**	https://support.apple.com/en-us/HT212713, https://support.apple.com/en-us/HT212622, https://support.apple.com/en-us/HT212623	O-APP-IPHO-051121/4132
Missing Authorization	19-Oct-21	2.9	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8, tvOS 15. An attacker in physical	https://support.apple.com/en-us/HT212819, https://supp	O-APP-IPHO-051121/4133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			proximity may be able to force a user onto a malicious Wi-Fi network during device setup. **CVE ID : CVE-2021-30810**	ort.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	2.1	This issue was addressed with improved checks. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8. A local attacker may be able to read sensitive information. **CVE ID : CVE-2021-30811**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212814	O-APP-IPHO-051121/4134
Exposure of Resource to Wrong Sphere	19-Oct-21	2.1	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management. This issue is fixed in iOS 15 and iPadOS 15. A local attacker may be able to view contacts from the lock screen. **CVE ID : CVE-2021-30815**	https://support.apple.com/en-us/HT212814	O-APP-IPHO-051121/4135
Out-of-bounds Read	19-Oct-21	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 15 and iPadOS 15. Processing a maliciously crafted USD file may disclose memory contents. **CVE ID : CVE-2021-30819**	https://support.apple.com/en-us/HT212814	O-APP-IPHO-051121/4136
N/A	19-Oct-21	7.5	A logic issue was addressed with improved state	https://support.apple.co	O-APP-IPHO-051121/4137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management. This issue is fixed in iOS 14.8 and iPadOS 14.8. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-30820**	m/en-us/HT212807	
N/A	19-Oct-21	4.6	This issue was addressed with improved checks. This issue is fixed in iOS 15 and iPadOS 15. A local attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-30825**	https://support.apple.com/en-us/HT212814	O-APP-IPHO-051121/4138
N/A	19-Oct-21	5	A logic issue was addressed with improved state management. This issue is fixed in iOS 15 and iPadOS 15. In certain situations, the baseband would fail to enable integrity and ciphering protection. **CVE ID : CVE-2021-30826**	https://support.apple.com/en-us/HT212814	O-APP-IPHO-051121/4139
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in Security Update 2021-005 Catalina, iTunes 12.12 for Windows, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30835**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212815,	O-APP-IPHO-051121/4140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	9.3	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8, tvOS 15. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-30837**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212814	O-APP-IPHO-051121/4141
N/A	19-Oct-21	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 15 and iPadOS 15. A malicious application may be able to execute arbitrary code with system privileges on devices with an Apple Neural Engine. **CVE ID : CVE-2021-30838**	https://support.apple.com/en-us/HT212814	O-APP-IPHO-051121/4142
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-	https://support.apple.com/en-us/HT212819,	O-APP-IPHO-051121/4143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30841**	https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30842**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://supp	O-APP-IPHO-051121/4144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30843**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com	O-APP-IPHO-051121/4145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				m/en-us/HT212814	
Out-of-bounds Write	19-Oct-21	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-30846**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212816, https://support.apple.com/en-us/HT212814	O-APP-IPHO-051121/4146
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in watchOS 8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30847**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.co	O-APP-IPHO-051121/4147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				m/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
Out-of-bounds Write	19-Oct-21	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, Safari 15, iOS 15 and iPadOS 15. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2021-30848**	https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212816, https://support.apple.com/en-us/HT212814	O-APP-IPHO-051121/4148
Out-of-bounds Write	19-Oct-21	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, watchOS 8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12	https://support.apple.com/en-us/HT212819, https://support.apple.co	O-APP-IPHO-051121/4149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-30849**	m/en-us/HT212817, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212816, https://support.apple.com/en-us/HT212814	
macos					
N/A	20-Oct-21	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM	https://www.oracle.com/security-alerts/cpuoct2021.html	O-APP-MACO-051121/4150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VirtualBox. Note: This vulnerability does not apply to Windows systems. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35538**		
N/A	19-Oct-21	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.5.1, iOS 14.7.1 and iPadOS 14.7.1, watchOS 7.6.1. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2021-30807**	https://support.apple.com/en-us/HT212713, https://support.apple.com/en-us/HT212622, https://support.apple.com/en-us/HT212623	O-APP-MACO-051121/4151
Improper Preservation of Permissions	19-Oct-21	4.6	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-30827**	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212805	O-APP-MACO-051121/4152
Exposure of Resource to Wrong Sphere	19-Oct-21	4.9	This issue was addressed with improved checks. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A local	https://support.apple.com/en-us/HT212804,	O-APP-MACO-051121/4153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user may be able to read arbitrary files as root. **CVE ID : CVE-2021-30828**	https://support.apple.com/en-us/HT212805	
Improper Privilege Management	19-Oct-21	4.6	A URI parsing issue was addressed with improved parsing. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A local user may be able to execute arbitrary files. **CVE ID : CVE-2021-30829**	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212805	O-APP-MACO-051121/4154
Out-of-bounds Write	19-Oct-21	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-30830**	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212805	O-APP-MACO-051121/4155
Out-of-bounds Write	19-Oct-21	4.6	A memory corruption issue was addressed with improved state management. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-30832**	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212805	O-APP-MACO-051121/4156
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur	https://support.apple.com/en-us/HT21281	O-APP-MACO-051121/4157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30841**	9, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30842**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804,	O-APP-MACO-051121/4158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30843**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://supp	O-APP-MACO-051121/4159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT212814	
N/A	19-Oct-21	5	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A remote attacker may be able to leak memory. **CVE ID : CVE-2021-30844**	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212805	O-APP-MACO-051121/4160
Out-of-bounds Read	19-Oct-21	4.9	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.6. A local user may be able to read kernel memory. **CVE ID : CVE-2021-30845**	https://support.apple.com/en-us/HT212804	O-APP-MACO-051121/4161
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in watchOS 8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30847**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT21281	O-APP-MACO-051121/4162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				5, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
Exposure of Resource to Wrong Sphere	19-Oct-21	7.1	An access issue was addressed with improved access restrictions. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6, tvOS 15. A user may gain access to protected parts of the file system. **CVE ID : CVE-2021-30850**	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805	O-APP-MACO-051121/4163
mac_os_x					
Improper Preservation of Permissions	19-Oct-21	4.6	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-30827**	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212805	O-APP-MAC_-051121/4164
Exposure of Resource to Wrong	19-Oct-21	4.9	This issue was addressed with improved checks. This issue is fixed in Security	https://support.apple.com/en-	O-APP-MAC_-051121/4165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			Update 2021-005 Catalina, macOS Big Sur 11.6. A local user may be able to read arbitrary files as root. **CVE ID : CVE-2021-30828**	us/HT212804, https://support.apple.com/en-us/HT212805	
Improper Privilege Management	19-Oct-21	4.6	A URI parsing issue was addressed with improved parsing. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A local user may be able to execute arbitrary files. **CVE ID : CVE-2021-30829**	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212805	O-APP-MAC_-051121/4166
Out-of-bounds Write	19-Oct-21	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-30830**	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212805	O-APP-MAC_-051121/4167
Out-of-bounds Write	19-Oct-21	4.6	A memory corruption issue was addressed with improved state management. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-30832**	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212805	O-APP-MAC_-051121/4168
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This	https://support.apple.co	O-APP-MAC_-051121/4169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in Security Update 2021-005 Catalina, iTunes 12.12 for Windows, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30835**	m/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30841**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-	O-APP-MAC_-051121/4170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30842**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT21281	O-APP-MAC_-051121/4171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30843**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	O-APP-MAC_-051121/4172
N/A	19-Oct-21	5	A logic issue was addressed with improved state management. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6. A remote attacker may be able to leak memory. **CVE ID : CVE-2021-30844**	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT21280	O-APP-MAC_-051121/4173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				5	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in watchOS 8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30847**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	O-APP-MAC_-051121/4174
Exposure of Resource to Wrong Sphere	19-Oct-21	7.1	An access issue was addressed with improved access restrictions. This issue is fixed in Security Update 2021-005 Catalina, macOS Big Sur 11.6, tvOS 15. A user may gain access to protected parts of the file system.	https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT21281	O-APP-MAC_-051121/4175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30850	5, https://support.apple.com/en-us/HT212805	
tvos					
Missing Authorization	19-Oct-21	2.9	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8, tvOS 15. An attacker in physical proximity may be able to force a user onto a malicious Wi-Fi network during device setup. **CVE ID : CVE-2021-30810**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212814	O-APP-TVOS-051121/4176
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in Security Update 2021-005 Catalina, iTunes 12.12 for Windows, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30835**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-	O-APP-TVOS-051121/4177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212805, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	9.3	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8, tvOS 15. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-30837**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212814	O-APP-TVOS-051121/4178
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30841**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-	O-APP-TVOS-051121/4179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30842**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT21281	O-APP-TVOS-051121/4180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30843**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	O-APP-TVOS-051121/4181
Out-of-bounds Write	19-Oct-21	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing maliciously crafted web content may lead to	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT21280	O-APP-TVOS-051121/4182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2021-30846**	7, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212816, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in watchOS 8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30847**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805,	O-APP-TVOS-051121/4183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212814	
Out-of-bounds Write	19-Oct-21	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, watchOS 8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-30849**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212816, https://support.apple.com/en-us/HT212814	O-APP-TVOS-051121/4184
Exposure of Resource to Wrong Sphere	19-Oct-21	7.1	An access issue was addressed with improved access restrictions. This issue is fixed in Security Update 2021-005 Catalina,	https://support.apple.com/en-us/HT212804,	O-APP-TVOS-051121/4185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			macOS Big Sur 11.6, tvOS 15. A user may gain access to protected parts of the file system. **CVE ID : CVE-2021-30850**	https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805	
watchos					
N/A	19-Oct-21	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.5.1, iOS 14.7.1 and iPadOS 14.7.1, watchOS 7.6.1. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2021-30807**	https://support.apple.com/en-us/HT212713, https://support.apple.com/en-us/HT212622, https://support.apple.com/en-us/HT212623	O-APP-WATC-051121/4186
Missing Authorization	19-Oct-21	2.9	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8, tvOS 15. An attacker in physical proximity may be able to force a user onto a malicious Wi-Fi network during device setup. **CVE ID : CVE-2021-30810**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT21281	O-APP-WATC-051121/4187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4	
N/A	19-Oct-21	2.1	This issue was addressed with improved checks. This issue is fixed in iOS 15 and iPadOS 15, watchOS 8. A local attacker may be able to read sensitive information. **CVE ID : CVE-2021-30811**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212814	O-APP-WATC-051121/4188
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in Security Update 2021-005 Catalina, iTunes 12.12 for Windows, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30835**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	O-APP-WATC-051121/4189
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur	https://support.apple.com/en-us/HT21281	O-APP-WATC-051121/4190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30841**	9, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30842**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804,	O-APP-WATC-051121/4191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing a maliciously crafted dfont file may lead to arbitrary code execution. **CVE ID : CVE-2021-30843**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://supp	O-APP-WATC-051121/4192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT212814	
Out-of-bounds Write	19-Oct-21	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, watchOS 8. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-30846**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212816, https://support.apple.com/en-us/HT212814	O-APP-WATC-051121/4193
N/A	19-Oct-21	6.8	This issue was addressed with improved checks. This issue is fixed in watchOS 8, macOS Big Sur 11.6, Security Update 2021-005 Catalina, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing a maliciously crafted image may lead to arbitrary code execution.	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://supp	O-APP-WATC-051121/4194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30847	ort.apple.com/en-us/HT212804, https://support.apple.com/en-us/HT212815, https://support.apple.com/en-us/HT212805, https://support.apple.com/en-us/HT212814	
Out-of-bounds Write	19-Oct-21	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, watchOS 8, Safari 15, tvOS 15, iOS 15 and iPadOS 15, iTunes 12.12 for Windows. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-30849**	https://support.apple.com/en-us/HT212819, https://support.apple.com/en-us/HT212817, https://support.apple.com/en-us/HT212807, https://support.apple.com/en-us/HT212815, https://support.apple.com	O-APP-WATC-051121/4195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				m/en-us/HT212816, https://support.apple.com/en-us/HT212814	
Arista					
eos					
Missing Encryption of Sensitive Data	21-Oct-21	4	On systems running Arista EOS and CloudEOS with the affected release version, when using shared secret profiles the password configured for use by BiDirectional Forwarding Detection (BFD) will be leaked when displaying output over eAPI or other JSON outputs to other authenticated users on the device. The affected EOS Versions are: all releases in 4.22.x train, 4.23.9 and below releases in the 4.23.x train, 4.24.7 and below releases in the 4.24.x train, 4.25.4 and below releases in the 4.25.x train, 4.26.1 and below releases in the 4.26.x train **CVE ID : CVE-2021-28496**	https://www.arista.com/en/support/advisories-notices/security-advisories/13243-security-advisory-0069	O-ARI-EOS-051121/4196
Asus					
ux582lr_firmware					
Incorrect Default Permissions	18-Oct-21	4.6	ASUSTek ZenBook Pro Due 15 UX582 laptop firmware through 203 has Insecure Permissions that allow	https://www.asus.com/Static_WebPage/ASUS-	O-ASU-UX58-051121/4197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks by a physically proximate attacker. **CVE ID : CVE-2021-42055**	Product-Security-Advisory/	
Cisco					
asa_5505_firmware					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	O-CIS-ASA_-051121/4198
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA)	https://tools.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-ASA_-051121/4199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**	visory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4201
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	O-CIS-ASA_-051121/4202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**		
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	O-CIS-ASA_-051121/4203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	O-CIS-ASA_-051121/4204
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	O-CIS-ASA_-051121/4205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**		
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	O-CIS-ASA_-051121/4206
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-	O-CIS-ASA_-051121/4207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**	g4cmrr7C	
asa_5512-x_firmware					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	O-CIS-ASA_-051121/4208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**		
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	O-CIS-ASA_-051121/4209
Improper Input	27-Oct-21	5	Multiple vulnerabilities in the Application Level	https://tools.cisco.com/se	O-CIS-ASA_-051121/4210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	O-CIS-ASA_-051121/4212
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	O-CIS-ASA_-051121/4213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**		
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	O-CIS-ASA_-051121/4214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	O-CIS-ASA_-051121/4215
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	O-CIS-ASA_-051121/4216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**		
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	O-CIS-ASA_-051121/4217
asa_5515-x_firmware					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco	https://tools.cisco.com/security/center	O-CIS-ASA_-051121/4218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**	/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	O-CIS-ASA_-051121/4219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4220
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the	https://tools.cisco.com/security/center	O-CIS-ASA_-051121/4221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	O-CIS-ASA_-051121/4222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**		
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	O-CIS-ASA_-051121/4223
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	O-CIS-ASA_-051121/4224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	O-CIS-ASA_-051121/4225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40117		
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	O-CIS-ASA_-051121/4226
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	O-CIS-ASA_-051121/4227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**		
asa_5525-x_firmware					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	O-CIS-ASA_-051121/4228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34783		
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	O-CIS-ASA_-051121/4229
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4231
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat	https://tools.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-ASA_-051121/4232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	visory/cisco-sa-asa-ftd-dos-Unk689XY	
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	O-CIS-ASA_-051121/4233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**		
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	O-CIS-ASA_-051121/4234
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-ASA_-051121/4235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	sa-asaftd-dos-4ygzLKU9	
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	O-CIS-ASA_-051121/4236
Uncontrolled Resource	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange	https://tools.cisco.com/se	O-CIS-ASA_-051121/4237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	
asa_5545-x_firmware					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	O-CIS-ASA_-051121/4238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**		
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	O-CIS-ASA_-051121/4239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4240
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	O-CIS-ASA_-051121/4242
Improper Enforcement of Message Integrity During Transmission	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-ASA_-051121/4243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
in a Communication Channel			transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**	sa-asa-ftd-dos-JxYWMJyL	
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	O-CIS-ASA_-051121/4244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	O-CIS-ASA_-051121/4245
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	O-CIS-ASA_-051121/4246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**		
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	O-CIS-ASA_-051121/4247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40125		
asa_5555-x_firmware					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	O-CIS-ASA_-051121/4248
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-	O-CIS-ASA_-051121/4249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**	ejjOgQEY	
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Slipstreaming. **CVE ID : CVE-2021-34790**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4251
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	O-CIS-ASA_-051121/4252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**		
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	O-CIS-ASA_-051121/4253
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality	https://tools.cisco.com/security/center/content/Cis	O-CIS-ASA_-051121/4254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**	coSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	O-CIS-ASA_-051121/4255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**		
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	O-CIS-ASA_-051121/4256
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	O-CIS-ASA_-051121/4257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**		
asa_5580_firmware					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M	O-CIS-ASA_-051121/4258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**		
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	O-CIS-ASA_-051121/4259
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-ASA_-051121/4260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	sa-natalg-bypass-cpKGqkng	
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	O-CIS-ASA_-051121/4262
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	O-CIS-ASA_-051121/4263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**		
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	O-CIS-ASA_-051121/4264
Uncontrolled	27-Oct-21	7.8	A vulnerability in SSL/TLS	https://tools.	O-CIS-ASA_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	051121/4265
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	O-CIS-ASA_-051121/4266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**		
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	O-CIS-ASA_-051121/4267
asa_5585-x_firmware					
Improper Input Validation	27-Oct-21	7.8	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-	O-CIS-ASA_-051121/4268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability. **CVE ID : CVE-2021-34783**	decrypt-dos-BMxYjm8M	
Improper Handling of Exceptional Conditions	27-Oct-21	4.3	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY	O-CIS-ASA_-051121/4269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts. **CVE ID : CVE-2021-34787**		
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34790**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng	O-CIS-ASA_-051121/4270
Improper Input Validation	27-Oct-21	5	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-	O-CIS-ASA_-051121/4271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming. **CVE ID : CVE-2021-34791**	bypass-cpKGqkng	
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-34792**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY	O-CIS-ASA_-051121/4272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	27-Oct-21	5	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption. **CVE ID : CVE-2021-34793**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL	O-CIS-ASA_-051121/4273
N/A	27-Oct-21	5	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3	O-CIS-ASA_-051121/4274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query. **CVE ID : CVE-2021-34794**		
Uncontrolled Resource Consumption	27-Oct-21	7.8	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40117**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9	O-CIS-ASA_-051121/4275
Improper Input Validation	27-Oct-21	7.1	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security	https://tools.cisco.com/security/center	O-CIS-ASA_-051121/4276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-40118**	/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA	
Uncontrolled Resource Consumption	27-Oct-21	6.3	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C	O-CIS-ASA_-051121/4277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device. **CVE ID : CVE-2021-40125**		
ios_xe_sd-wan					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-21	6.9	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2021-1529**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A	O-CIS-IOS_-051121/4278
commscope					
arris_surfboard_sb8200_firmware					
Cross-Site Request Forgery (CSRF)	21-Oct-21	6.8	The administration web interface for the Arris Surfboard SB8200 lacks any protections against cross-site request forgery attacks. This means that an attacker could make configuration changes (such as changing the administrative	N/A	O-COM-ARRI-051121/4279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			password) without the consent of the user. **CVE ID : CVE-2021-20120**		
D-link					
dap-2020_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-21	3.3	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the getpage parameter provided to the webproc endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-12103. **CVE ID : CVE-2021-34860**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201	O-D-L-DAP--051121/4280
Stack-based Buffer Overflow	25-Oct-21	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the webproc endpoint, which listens on TCP port 80 by default. The issue results	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201	O-D-L-DAP--051121/4281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-12104. **CVE ID : CVE-2021-34861**		
Stack-based Buffer Overflow	25-Oct-21	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the var:menu parameter provided to the webproc endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13270. **CVE ID : CVE-2021-34862**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201	O-D-L-DAP--051121/4282
Stack-based Buffer Overflow	25-Oct-21	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201	O-D-L-DAP--051121/4283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flaw exists within the handling of the var:page parameter provided to the webproc endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13271. **CVE ID : CVE-2021-34863**		
Debian					
debian_linux					
Integer Overflow or Wraparound	18-Oct-21	5	The gmp plugin in strongSwan before 5.9.4 has a remote integer overflow via a crafted certificate with an RSASSA-PSS signature. For example, this can be triggered by an unrelated self-signed CA certificate sent by an initiator. Remote code execution cannot occur. **CVE ID : CVE-2021-41990**	https://www.strongswan.org/blog/2021/10/18/strongswan-vulnerability-(cve-2021-41990).html	O-DEB-DEBI-051121/4284
Integer Overflow or Wraparound	18-Oct-21	5	The in-memory certificate cache in strongSwan before 5.9.4 has a remote integer overflow upon receiving many requests with different certificates to fill the cache and later trigger the replacement of cache entries. The code attempts to select a less-often-used cache entry by means of a random number generator,	https://www.strongswan.org/blog/2021/10/18/strongswan-vulnerability-(cve-2021-41991).html	O-DEB-DEBI-051121/4285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			but this is not done correctly. Remote code execution might be a slight possibility. **CVE ID : CVE-2021-41991**		
Improper Restriction of Excessive Authentication Attempts	21-Oct-21	6.8	GNU Mailman before 2.1.35 may allow remote Privilege Escalation. A certain csrf_token value is derived from the admin password, and may be useful in conducting a brute-force attack against that password. **CVE ID : CVE-2021-42096**	https://mail.python.org/archives/list/mailman-announce@python.org/thread/IKCO6JU755AP5G5TKMBJL6IEZQTTNPDQ/, https://bugs.launchpad.net/mailman/+bug/1947639, http://www.openwall.com/lists/oss-security/2021/10/21/4	O-DEB-DEBI-051121/4286
Cross-Site Request Forgery (CSRF)	21-Oct-21	9.3	GNU Mailman before 2.1.35 may allow remote Privilege Escalation. A csrf_token value is not specific to a single user account. An attacker can obtain a value within the context of an unprivileged user account, and then use that value in a CSRF attack against an admin (e.g., for account takeover). **CVE ID : CVE-2021-42097**	https://mail.python.org/archives/list/mailman-announce@python.org/thread/IKCO6JU755AP5G5TKMBJL6IEZQTTNPDQ/, https://bugs.launchpad.net/mailman/+bug/1947640,	O-DEB-DEBI-051121/4287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				http://www.openwall.com/lists/oss-security/2021/10/21/4	
Out-of-bounds Write	25-Oct-21	7.2	In PHP versions 7.3.x up to and including 7.3.31, 7.4.x below 7.4.25 and 8.0.x below 8.0.12, when running PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower-privileged users, it is possible for the child processes to access memory shared with the main process and write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and writes, which can be used to escalate privileges from local unprivileged user to the root user. **CVE ID : CVE-2021-21703**	https://bugs.php.net/bug.php?id=81026	O-DEB-DEBI-051121/4288
Emerson					
wireless_1410d_gateway_firmware					
Improper Input Validation	22-Oct-21	6.5	The affected product is vulnerable to improper input validation in the restore file. This enables an attacker to provide malicious config files to replace any file on disk. **CVE ID : CVE-2021-38485**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4289
Exposure of Resource to	22-Oct-21	4	The affected product is vulnerable to a disclosure of	https://us-cert.cisa.gov/	O-EME-WIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			peer username and password by allowing all users access to read global variables. **CVE ID : CVE-2021-42536**	ics/advisories/icsa-21-278-02	051121/4290
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Oct-21	6.5	The affected product is vulnerable to a parameter injection via passphrase, which enables the attacker to supply uncontrolled input. **CVE ID : CVE-2021-42538**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4291
Missing Authentication for Critical Function	22-Oct-21	6.5	The affected product is vulnerable to a missing permission validation on system backup restore, which could lead to account take over and unapproved settings change. **CVE ID : CVE-2021-42539**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4292
Write-what-where Condition	22-Oct-21	6.5	The affected product is vulnerable to a unsanitized extract folder for system configuration. A low-privileged user can leverage this logic to overwrite the settings and other key functionality. **CVE ID : CVE-2021-42540**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4293
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Oct-21	6.5	The affected product is vulnerable to directory traversal due to mishandling of provided backup folder structure. **CVE ID : CVE-2021-42542**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wireless_1410_gateway_firmware					
Improper Input Validation	22-Oct-21	6.5	The affected product is vulnerable to improper input validation in the restore file. This enables an attacker to provide malicious config files to replace any file on disk. **CVE ID : CVE-2021-38485**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4295
Exposure of Resource to Wrong Sphere	22-Oct-21	4	The affected product is vulnerable to a disclosure of peer username and password by allowing all users access to read global variables. **CVE ID : CVE-2021-42536**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4296
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Oct-21	6.5	The affected product is vulnerable to a parameter injection via passphrase, which enables the attacker to supply uncontrolled input. **CVE ID : CVE-2021-42538**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4297
Missing Authentication for Critical Function	22-Oct-21	6.5	The affected product is vulnerable to a missing permission validation on system backup restore, which could lead to account take over and unapproved settings change. **CVE ID : CVE-2021-42539**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4298
Write-what-where Condition	22-Oct-21	6.5	The affected product is vulnerable to a unsanitized extract folder for system configuration. A low-privileged user can leverage this logic to overwrite the	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings and other key functionality. **CVE ID : CVE-2021-42540**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Oct-21	6.5	The affected product is vulnerable to directory traversal due to mishandling of provided backup folder structure. **CVE ID : CVE-2021-42542**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4300
wireless_1420_gateway_firmware					
Improper Input Validation	22-Oct-21	6.5	The affected product is vulnerable to improper input validation in the restore file. This enables an attacker to provide malicious config files to replace any file on disk. **CVE ID : CVE-2021-38485**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4301
Exposure of Resource to Wrong Sphere	22-Oct-21	4	The affected product is vulnerable to a disclosure of peer username and password by allowing all users access to read global variables. **CVE ID : CVE-2021-42536**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4302
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Oct-21	6.5	The affected product is vulnerable to a parameter injection via passphrase, which enables the attacker to supply uncontrolled input. **CVE ID : CVE-2021-42538**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4303
Missing Authentication for Critical	22-Oct-21	6.5	The affected product is vulnerable to a missing permission validation on	https://us-cert.cisa.gov/ics/advisorie	O-EME-WIRE-051121/4304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			system backup restore, which could lead to account take over and unapproved settings change. **CVE ID : CVE-2021-42539**	s/icsa-21-278-02	
Write-what-where Condition	22-Oct-21	6.5	The affected product is vulnerable to a unsanitized extract folder for system configuration. A low-privileged user can leverage this logic to overwrite the settings and other key functionality. **CVE ID : CVE-2021-42540**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4305
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Oct-21	6.5	The affected product is vulnerable to directory traversal due to mishandling of provided backup folder structure. **CVE ID : CVE-2021-42542**	https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02	O-EME-WIRE-051121/4306
Fedoraproject					
fedora					
Incorrect Authorization	20-Oct-21	7.1	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	O-FED-FEDO-051121/4307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-35550**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Utility). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	O-FED-FEDO-051121/4308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35561**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Keytool). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory/ntap-20211022-0004/	O-FED-FEDO-051121/4309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-35564**		
N/A	20-Oct-21	5	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpuoct2021.html, https://security.netapp.com/advisory	O-FED-FEDO-051121/4310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-35565**	/ntap-20211022-0004/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-Oct-21	7.1	A flaw was found in the libtpms code that may cause access beyond the boundary of internal buffers. The vulnerability is triggered by specially-crafted TPM2 command packets that then trigger the issue when the state of the TPM2's volatile state is written. The highest threat from this vulnerability is to system availability. This issue affects	https://bugzilla.redhat.com/show_bug.cgi?id=1998588	O-FED-FEDO-051121/4311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			libtpms versions before 0.8.5, before 0.7.9 and before 0.6.6. **CVE ID : CVE-2021-3746**		
Heap-based Buffer Overflow	19-Oct-21	6.8	vim is vulnerable to Heap-based Buffer Overflow **CVE ID : CVE-2021-3872**	https://github.com/vim/vim/commit/826bfe4bbd7594188e3d74d2539d9707b1c6a14b, https://huntr.dev/bounties/c958013b-1c09-4939-92ca-92f50aa169e8	O-FED-FEDO-051121/4312
Google					
android					
Out-of-bounds Read	25-Oct-21	2.1	In flv extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561359; Issue ID: ALPS05561359. **CVE ID : CVE-2021-0409**	N/A	O-GOO-ANDR-051121/4313
Out-of-bounds Read	25-Oct-21	2.1	In flv extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User	N/A	O-GOO-ANDR-051121/4314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05561360; Issue ID: ALPS05561360. **CVE ID : CVE-2021-0410**		
Out-of-bounds Read	25-Oct-21	2.1	In flv extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561362; Issue ID: ALPS05561362. **CVE ID : CVE-2021-0411**	N/A	O-GOO-ANDR-051121/4315
Out-of-bounds Read	25-Oct-21	2.1	In flv extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561366; Issue ID: ALPS05561366. **CVE ID : CVE-2021-0412**	N/A	O-GOO-ANDR-051121/4316
Out-of-bounds Read	25-Oct-21	2.1	In flv extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561379; Issue ID:	N/A	O-GOO-ANDR-051121/4317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05561379. **CVE ID : CVE-2021-0413**		
Out-of-bounds Read	25-Oct-21	2.1	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561384; Issue ID: ALPS05561384. **CVE ID : CVE-2021-0414**	N/A	O-GOO-ANDR-051121/4318
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Oct-21	4.4	In multiple methods of AAudioService, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-153358911 **CVE ID : CVE-2021-0483**	https://source.android.com/security/bulletin/2021-10-01	O-GOO-ANDR-051121/4319
Out-of-bounds Read	25-Oct-21	2.1	In asf extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05489178.	N/A	O-GOO-ANDR-051121/4320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0613		
Out-of-bounds Read	25-Oct-21	2.1	In asf extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05495528; Issue ID: ALPS05495528. **CVE ID : CVE-2021-0614**	N/A	O-GOO-ANDR-051121/4321
Out-of-bounds Read	25-Oct-21	2.1	In flv extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561369; Issue ID: ALPS05561369. **CVE ID : CVE-2021-0615**	N/A	O-GOO-ANDR-051121/4322
Out-of-bounds Read	25-Oct-21	2.1	In ape extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561389; Issue ID: ALPS05561389. **CVE ID : CVE-2021-0616**	N/A	O-GOO-ANDR-051121/4323
Out-of-bounds Read	25-Oct-21	2.1	In ape extractor, there is a possible out of bounds read	N/A	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561391; Issue ID: ALPS05561391. **CVE ID : CVE-2021-0617**		051121/4324
Out-of-bounds Read	25-Oct-21	2.1	In ape extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561394; Issue ID: ALPS05561394. **CVE ID : CVE-2021-0618**	N/A	O-GOO-ANDR-051121/4325
Improper Locking	25-Oct-21	7.2	In ccu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594996; Issue ID: ALPS05594996. **CVE ID : CVE-2021-0625**	N/A	O-GOO-ANDR-051121/4326
Integer Overflow or Wraparound	25-Oct-21	5	In wifi driver, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed.	N/A	O-GOO-ANDR-051121/4327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05551397; Issue ID: ALPS05551397. **CVE ID : CVE-2021-0630**		
Out-of-bounds Read	25-Oct-21	5	In wifi driver, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05551435; Issue ID: ALPS05551435. **CVE ID : CVE-2021-0631**	N/A	O-GOO-ANDR-051121/4328
Out-of-bounds Read	25-Oct-21	3.3	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker under certain build conditions with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05560246; Issue ID: ALPS05551383. **CVE ID : CVE-2021-0632**	N/A	O-GOO-ANDR-051121/4329
Out-of-bounds Write	25-Oct-21	7.2	In display driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	N/A	O-GOO-ANDR-051121/4330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05585423; Issue ID: ALPS05585423. **CVE ID : CVE-2021-0633**		
Use of Uninitialized Resource	25-Oct-21	7.2	In display driver, there is a possible memory corruption due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594994; Issue ID: ALPS05594994. **CVE ID : CVE-2021-0634**	N/A	O-GOO-ANDR-051121/4331
Missing Authorization	22-Oct-21	2.1	In getAllSubInfoList of SubscriptionController.java, there is a possible way to retrieve a long term identifier without the correct permissions due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-183612370 **CVE ID : CVE-2021-0643**	https://source.android.com/security/bulletin/2021-10-01	O-GOO-ANDR-051121/4332
Improper Input Validation	22-Oct-21	4.7	In loadLabel of PackageItemInfo.java, there is a possible way to DoS a device by having a long label in an app due to incorrect input validation. This could lead to local denial of service	https://source.android.com/security/bulletin/2021-10-01	O-GOO-ANDR-051121/4333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-9 Android-10Android ID: A-67013844 **CVE ID : CVE-2021-0651**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-21	7.2	In VectorDrawable::VectorDrawable of VectorDrawable.java, there is a possible way to introduce a memory corruption due to sharing of not thread-safe objects. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-185178568 **CVE ID : CVE-2021-0652**	https://source.android.com/security/bulletin/2021-10-01	O-GOO-ANDR-051121/4334
Out-of-bounds Write	25-Oct-21	7.2	In audio DSP, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05844413; Issue ID: ALPS05844413. **CVE ID : CVE-2021-0661**	N/A	O-GOO-ANDR-051121/4335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Oct-21	7.2	In audio DSP, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05844434; Issue ID: ALPS05844434. **CVE ID : CVE-2021-0662**	N/A	O-GOO-ANDR-051121/4336
Out-of-bounds Write	25-Oct-21	7.2	In audio DSP, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05844458; Issue ID: ALPS05844458. **CVE ID : CVE-2021-0663**	N/A	O-GOO-ANDR-051121/4337
N/A	22-Oct-21	1.9	In RevertActiveSessions of apexd.cpp, there is a possible way to share the wrong file due to an unintentional MediaStore downgrade. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-193932765 **CVE ID : CVE-2021-0702**	https://source.android.com/security/bulletin/2021-10-01	O-GOO-ANDR-051121/4338
Use After	22-Oct-21	7.2	In SecondStageMain of	https://sour	O-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			init.cpp, there is a possible use after free due to incorrect shared_ptr usage. This could lead to local escalation of privilege if the attacker has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-184569329 **CVE ID : CVE-2021-0703**	ce.android.com/security/bulletin/2021-10-01	ANDR-051121/4339
Improper Privilege Management	22-Oct-21	7.2	In sanitizeSbn of NotificationManagerService.java, there is a possible way to keep service running in foreground and keep granted permissions due to Bypass of Background Service Restrictions. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-185388103 **CVE ID : CVE-2021-0705**	https://source.android.com/security/bulletin/2021-10-01	O-GOO-ANDR-051121/4340
Incorrect Default Permissions	22-Oct-21	4.9	In startListening of PluginManagerImpl.java, there is a possible way to disable arbitrary app components due to a missing permission check. This could lead to local denial of service with no additional execution	https://source.android.com/security/bulletin/2021-10-01	O-GOO-ANDR-051121/4341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-193444889 **CVE ID : CVE-2021-0706**		
Externally Controlled Reference to a Resource in Another Sphere	22-Oct-21	7.2	In runDumpHeap of ActivityManagerShellCommand.java, there is a possible deletion of system files due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-183262161 **CVE ID : CVE-2021-0708**	https://source.android.com/security/bulletin/2021-10-01	O-GOO-ANDR-051121/4342
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Oct-21	9.3	In RW_SetActivatedTagType of rw_main.cc, there is possible memory corruption due to a race condition. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-192472262 **CVE ID : CVE-2021-0870**	https://source.android.com/security/bulletin/2021-10-01	O-GOO-ANDR-051121/4343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Oct-21	7.2	In ip6_xmit of ip6_output.c, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-168607263References: Upstream kernel **CVE ID : CVE-2021-0935**	https://source.android.com/security/bulletin/pixel/2021-10-01	O-GOO-ANDR-051121/4344
Use After Free	25-Oct-21	4.6	In acc_read of f_accessory.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-173789633References: Upstream kernel **CVE ID : CVE-2021-0936**	https://source.android.com/security/bulletin/pixel/2021-10-01	O-GOO-ANDR-051121/4345
Use of Uninitialized Resource	25-Oct-21	2.1	In memzero_explicit of compiler-clang.h, there is a possible bypass of defense in depth due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-	https://source.android.com/security/bulletin/pixel/2021-10-01	O-GOO-ANDR-051121/4346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			171418586References: Upstream kernel **CVE ID : CVE-2021-0938**		
Out-of-bounds Read	25-Oct-21	2.1	In set_default_passthru_cfg of passthru.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-186026549References: N/A **CVE ID : CVE-2021-0939**	https://source.android.com/security/bulletin/pixel/2021-10-01	O-GOO-ANDR-051121/4347
Out-of-bounds Write	25-Oct-21	7.2	In TBD of TBD, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-171315276References: N/A **CVE ID : CVE-2021-0940**	https://source.android.com/security/bulletin/pixel/2021-10-01	O-GOO-ANDR-051121/4348
Out-of-bounds Read	25-Oct-21	7.2	In bpf_skb_change_head of filter.c, there is a possible out of bounds read due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not	https://source.android.com/security/bulletin/pixel/2021-10-01	O-GOO-ANDR-051121/4349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-154177719References: Upstream kernel **CVE ID : CVE-2021-0941**		
hpe					
superdome_flex_280_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	4.3	A potential security vulnerability has been identified in HPE Superdome Flex Servers. The vulnerability could be remotely exploited to allow Cross Site Scripting (XSS) because the Session Cookie is missing an HttpOnly Attribute. HPE has provided a firmware update to resolve the vulnerability in HPE Superdome Flex Servers. **CVE ID : CVE-2021-26589**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04199en_us	O-HPE-SUPE-051121/4350
superdome_flex_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	4.3	A potential security vulnerability has been identified in HPE Superdome Flex Servers. The vulnerability could be remotely exploited to allow Cross Site Scripting (XSS) because the Session Cookie is missing an HttpOnly Attribute. HPE has provided a firmware update to resolve the vulnerability in HPE Superdome Flex Servers. **CVE ID : CVE-2021-26589**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04199en_us	O-HPE-SUPE-051121/4351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Huawei					
cloudengine_12800_firmware					
Use After Free	27-Oct-21	3.3	There is a use-after-free (UAF) vulnerability in Huawei products. An attacker may craft specific packets to exploit this vulnerability. Successful exploitation may cause the service abnormal. Affected product versions include:CloudEngine 12800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 5800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 6800 V200R005C10SPC800,V200R005C20SPC800,V200R019C00SPC800;CloudEngine 7800 V200R005C10SPC800,V200R019C00SPC800. **CVE ID : CVE-2021-37122**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211008-01-cloudengine-en	O-HUA-CLOU-051121/4352
cloudengine_5800_firmware					
Use After Free	27-Oct-21	3.3	There is a use-after-free (UAF) vulnerability in Huawei products. An attacker may craft specific packets to exploit this vulnerability. Successful exploitation may cause the service abnormal. Affected product versions include:CloudEngine 12800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 5800	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211008-01-cloudengine-en	O-HUA-CLOU-051121/4353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R005C10SPC800,V200R019C00SPC800;CloudEngine 6800 V200R005C10SPC800,V200R005C20SPC800,V200R019C00SPC800;CloudEngine 7800 V200R005C10SPC800,V200R019C00SPC800. **CVE ID : CVE-2021-37122**		
cloudengine_6800_firmware					
Use After Free	27-Oct-21	3.3	There is a use-after-free (UAF) vulnerability in Huawei products. An attacker may craft specific packets to exploit this vulnerability. Successful exploitation may cause the service abnormal. Affected product versions include:CloudEngine 12800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 5800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 6800 V200R005C10SPC800,V200R005C20SPC800,V200R019C00SPC800;CloudEngine 7800 V200R005C10SPC800,V200R019C00SPC800. **CVE ID : CVE-2021-37122**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211008-01-cloudengine-en	O-HUA-CLOU-051121/4354
cloudengine_7800_firmware					
Use After Free	27-Oct-21	3.3	There is a use-after-free (UAF) vulnerability in Huawei products. An attacker may craft specific	https://www.huawei.com/en/psirt/security-	O-HUA-CLOU-051121/4355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets to exploit this vulnerability. Successful exploitation may cause the service abnormal. Affected product versions include:CloudEngine 12800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 5800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 6800 V200R005C10SPC800,V200R005C20SPC800,V200R019C00SPC800;CloudEngine 7800 V200R005C10SPC800,V200R019C00SPC800. **CVE ID : CVE-2021-37122**	advisories/huawei-sa-20211008-01-cloudengine-en	
emui					
N/A	28-Oct-21	5	There is a Remote DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability can affect service integrity. **CVE ID : CVE-2021-22401**	https://consumer.huawei.com/en/support/bulletin/2021/7/	O-HUA-EMUI-051121/4356
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Oct-21	5	There is a Directory traversal vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-22404**	https://consumer.huawei.com/en/support/bulletin/2021/7/	O-HUA-EMUI-051121/4357
N/A	28-Oct-21	5	There is a Configuration defects in Huawei Smartphone.Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin	O-HUA-EMUI-051121/4358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may affect service availability. **CVE ID : CVE-2021-22405**	/2021/7/	
fusioncube_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Oct-21	5	There is a path traversal vulnerability in Huawei FusionCube 6.0.2.The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. **CVE ID : CVE-2021-37130**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-pathtraversal-en	O-HUA-FUSI-051121/4359
harmonyos					
Improper Input Validation	28-Oct-21	2.1	A component of the HarmonyOS has a Improper Input Validation vulnerability. Local attackers may exploit this vulnerability to read at any address. **CVE ID : CVE-2021-22452**	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202107-0000001123874808	O-HUA-HARM-051121/4360
Improper Input Validation	28-Oct-21	2.1	A component of the HarmonyOS has a Improper Input Validation vulnerability. Local attackers may exploit this vulnerability to cause nearby	https://device.harmonyos.com/cn/docs/security/update/security-bulletins-	O-HUA-HARM-051121/4361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process crash. **CVE ID : CVE-2021-22453**	202107-0000001123874808	
imanager_neteco_6000_firmware					
Improper Verification of Cryptographic Signature	27-Oct-21	9	There is a signature management vulnerability in some huawei products. An attacker can forge signature and bypass the signature check. During firmware update process, successful exploit this vulnerability can cause the forged system file overwrite the correct system file. Affected product versions include:iManager NetEco V600R010C00CP2001,V600R010C00CP2002,V600R010C00SPC100,V600R010C00SPC110,V600R010C00SPC120,V600R010C00SPC200,V600R010C00SPC210,V600R010C00SPC300;iManager NetEco 6000 V600R009C00SPC100,V600R009C00SPC110,V600R009C00SPC120,V600R009C00SPC190,V600R009C00SPC200,V600R009C00SPC201,V600R009C00SPC202,V600R009C00SPC210. **CVE ID : CVE-2021-37127**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-signature-en	O-HUA-IMAN-051121/4362
imanager_neteco_firmware					
Improper Verification of Cryptographic Signature	27-Oct-21	9	There is a signature management vulnerability in some huawei products. An attacker can forge signature and bypass the signature	https://www.huawei.com/en/psirt/security-advisories/h	O-HUA-IMAN-051121/4363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check. During firmware update process, successful exploit this vulnerability can cause the forged system file overwrite the correct system file. Affected product versions include:iManager NetEco V600R010C00CP2001,V600R010C00CP2002,V600R010C00SPC100,V600R010C00SPC110,V600R010C00SPC120,V600R010C00SPC200,V600R010C00SPC210,V600R010C00SPC300;iManager NetEco 6000 V600R009C00SPC100,V600R009C00SPC110,V600R009C00SPC120,V600R009C00SPC190,V600R009C00SPC200,V600R009C00SPC201,V600R009C00SPC202,V600R009C00SPC210. **CVE ID : CVE-2021-37127**	uawei-sa-20211020-01-signature-en	
ips_module_firmware					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	O-HUA-IPS_-051121/4364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
magic_ui					
N/A	28-Oct-21	5	There is a Remote DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability can affect service integrity.	https://consumer.huawei.com/en/support/bulletin/2021/7/	O-HUA-MAGI-051121/4365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22401		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Oct-21	5	There is a Directory traversal vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2021-22404**	https://consumer.huawei.com/en/support/bulletin/2021/7/	O-HUA-MAGI-051121/4366
N/A	28-Oct-21	5	There is a Configuration defects in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability. **CVE ID : CVE-2021-22405**	https://consumer.huawei.com/en/support/bulletin/2021/7/	O-HUA-MAGI-051121/4367
ngfw_module_firmware					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V20	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	O-HUA-NGFW-051121/4368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
nip6600_firmware					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C2	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	O-HUA-NIP6-051121/4369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s12700_firmware					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a	https://www.huawei.com/en/psirt/security-	O-HUA-S127-051121/4370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500	advisories/huawei-sa-20211020-01-outofwrite-en	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s1700_firmware					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	O-HUA-S170-051121/4371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s2700_firmware					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	O-HUA-S270-051121/4372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s5700_firmware					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	O-HUA-S570-051121/4373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s6700_firmware					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-	O-HUA-S670-051121/4374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**	en	
s7700_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10S	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	O-HUA-S770-051121/4375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
s9700_firmware					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R020C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	O-HUA-S970-051121/4376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
usg9500_firmware					
Out-of-bounds Write	27-Oct-21	5	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC200,V200R019C00SPC500,V200R019C10SPC200,V200R02	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en	O-HUA-USG9-051121/4377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0C00,V200R020C10;S1700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC500;S6700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20. **CVE ID : CVE-2021-37129**		
IBM					
flashsystem_9000_firmware					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force ID: 206229. **CVE ID : CVE-2021-29873**	https://www.ibm.com/support/pages/node/6497111, https://www.ibm.com/support/pages/node/6507091, https://exchange.xforce.ibmcloud.com	O-IBM-FLAS-051121/4378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/vulnerabilities/206229	
flashsystem_9100_firmware					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force ID: 206229. **CVE ID : CVE-2021-29873**	https://www.ibm.com/support/pages/node/6497111, https://www.ibm.com/support/pages/node/6507091, https://exchange.xforce.ibmcloud.com/vulnerabilities/206229	O-IBM-FLAS-051121/4379
san_volume_controller_firmware					
Exposure of Resource to Wrong Sphere	21-Oct-21	5.5	IBM Flash System 900 could allow an authenticated attacker to obtain sensitive information and cause a denial of service due to a restricted shell escape vulnerability. IBM X-Force ID: 206229. **CVE ID : CVE-2021-29873**	https://www.ibm.com/support/pages/node/6497111, https://www.ibm.com/support/pages/node/6507091, https://exchange.xforce.ibmcloud.com/vulnerabilities/206229	O-IBM-SAN_-051121/4380
inhandnetworks					
ir615_firmware					
Weak Password	19-Oct-21	7.5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870	N/A	O-INH-IR61-051121/4381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Requirements			does not enforce an efficient password policy. This may allow an attacker with obtained user credentials to enumerate passwords and impersonate other application users and perform operations on their behalf. **CVE ID : CVE-2021-38462**		
Inadequate Encryption Strength	19-Oct-21	5.8	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 have inadequate encryption strength, which may allow an attacker to intercept the communication and steal sensitive information or hijack the session. **CVE ID : CVE-2021-38464**	N/A	O-INH-IR61-051121/4382
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	4.3	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 do not perform sufficient input validation on client requests from the help page. This may allow an attacker to perform a reflected cross-site scripting attack, which could allow an attacker to run code on behalf of the client browser. **CVE ID : CVE-2021-38466**	N/A	O-INH-IR61-051121/4383
Improper Neutralization of Input During Web Page Generation	19-Oct-21	3.5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 are vulnerable to stored cross-scripting, which may allow an attacker to hijack	N/A	O-INH-IR61-051121/4384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			sessions of users connected to the system. **CVE ID : CVE-2021-38468**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-21	6.5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 are vulnerable to an attacker using a ping tool to inject commands into the device. This may allow the attacker to remotely run commands on behalf of the device. **CVE ID : CVE-2021-38470**	N/A	O-INH-IR61-051121/4385
Improper Restriction of Rendered UI Layers or Frames	19-Oct-21	4.3	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 management portal does not contain an X-FRAME-OPTIONS header, which an attacker may take advantage of by sending a link to an administrator that frames the router's management portal and could lure the administrator to perform changes. **CVE ID : CVE-2021-38472**	N/A	O-INH-IR61-051121/4386
Improper Restriction of Excessive Authentication Attempts	19-Oct-21	5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 have has no account lockout policy configured for the login page of the product. This may allow an attacker to execute a brute-force password attack with no time limitation and without harming the normal operation of the user. This	N/A	O-INH-IR61-051121/4387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to gain valid credentials for the product interface. **CVE ID : CVE-2021-38474**		
Observable Discrepancy	19-Oct-21	5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 authentication process response indicates and validates the existence of a username. This may allow an attacker to enumerate different user accounts. **CVE ID : CVE-2021-38476**	N/A	O-INH-IR61-051121/4388
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-21	6.5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 are vulnerable to an attacker using a traceroute tool to inject commands into the device. This may allow the attacker to remotely run commands on behalf of the device. **CVE ID : CVE-2021-38478**	N/A	O-INH-IR61-051121/4389
Cross-Site Request Forgery (CSRF)	19-Oct-21	9.3	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 are vulnerable to cross-site request forgery when unauthorized commands are submitted from a user the web application trusts. This may allow an attacker to remotely perform actions on the router's management portal, such as making configuration changes, changing administrator	N/A	O-INH-IR61-051121/4390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials, and running system commands on the router. **CVE ID : CVE-2021-38480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 website used to control the router is vulnerable to stored cross-site scripting, which may allow an attacker to hijack sessions of users connected to the system. **CVE ID : CVE-2021-38482**	N/A	O-INH-IR61-051121/4391
Unrestricted Upload of File with Dangerous Type	19-Oct-21	9	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 do not have a filter or signature check to detect or prevent an upload of malicious files to the server, which may allow an attacker, acting as an administrator, to upload malicious files. This could result in cross-site scripting, deletion of system files, and remote code execution. **CVE ID : CVE-2021-38484**	N/A	O-INH-IR61-051121/4392
Improper Authorization	19-Oct-21	6	InHand Networks IR615 Router's Versions 2.3.0.r4724 and 2.3.0.r4870 cloud portal allows for self-registration of the affected product without any requirements to create an account, which may allow an attacker to have full control over the product and	N/A	O-INH-IR61-051121/4393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute code within the internal network to which the product is connected. **CVE ID : CVE-2021-38486**		
Juniper					
128_technology_session_smart_router_firmware					
Improper Authentication	19-Oct-21	7.5	The usage of an internal HTTP header created an authentication bypass vulnerability (CWE-287), allowing an attacker to view internal files, change settings, manipulate services and execute arbitrary code. This issue affects all Juniper Networks 128 Technology Session Smart Router versions prior to 4.5.11, and all versions of 5.0 up to and including 5.0.1. **CVE ID : CVE-2021-31349**	https://kb.juniper.net/JSA11256	O-JUN-128_-051121/4394
junos					
Improper Handling of Exceptional Conditions	19-Oct-21	7.1	An Improper Handling of Exceptional Conditions vulnerability in the processing of a transit or directly received malformed IPv6 packet in Juniper Networks Junos OS results in a kernel crash, causing the device to restart, leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects systems with IPv6 configured. Devices with only IPv4	https://kb.juniper.net/JSA11213	O-JUN-JUNO-051121/4395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configured are not vulnerable to this issue. This issue affects Juniper Networks Junos OS: 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S1, 20.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 19.4R1. **CVE ID : CVE-2021-0299**		
Improper Privilege Management	19-Oct-21	9	An Improper Privilege Management vulnerability in the gRPC framework, used by the Juniper Extension Toolkit (JET) API on Juniper Networks Junos OS and Junos OS Evolved, allows a network-based, low-privileged authenticated attacker to perform operations as root, leading to complete compromise of the targeted system. The issue is caused by the JET service daemon (jsd) process authenticating the user, then passing configuration operations directly to the management daemon (mgd) process, which runs as root. This issue affects Juniper Networks Junos OS: 18.4 versions prior to 18.4R1-S8, 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R2-S3, 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to	https://kb.juniper.net/JSA11215	O-JUN-JUNO-051121/4396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. **CVE ID : CVE-2021-31350**		
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions in packet processing on the MS-MPC/MS-MIC utilized by Juniper Networks Junos OS allows a malicious attacker to send a specific packet, triggering the MS-MPC/MS-MIC to reset, causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects specific versions of Juniper Networks Junos OS on MX Series: 17.3R3-S11; 17.4R2-S13; 17.4R3 prior to 17.4R3-S5; 18.1R3-S12; 18.2R2-S8, 18.2R3-S7, 18.2R3-S8; 18.3R3-S4; 18.4R3-S7;	https://kb.juniper.net/JSA11216	O-JUN-JUNO-051121/4397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.1R3-S4, 19.1R3-S5; 19.2R1-S6; 19.3R3-S2; 19.4R2-S4, 19.4R2-S5; 19.4R3-S2; 20.1R2-S1; 20.2R2-S2, 20.2R2-S3, 20.2R3; 20.3R2, 20.3R2-S1; 20.4R1, 20.4R1-S1, 20.4R2; 21.1R1; This issue does not affect any version of Juniper Networks Junos OS prior to 15.1X49-D240; **CVE ID : CVE-2021-31351**		
Improper Handling of Exceptional Conditions	19-Oct-21	5	An Improper Handling of Exceptional Conditions vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an attacker to inject a specific BGP update, causing the routing protocol daemon (RPD) to crash and restart, leading to a Denial of Service (DoS). Continued receipt and processing of the BGP update will create a sustained Denial of Service (DoS) condition. This issue affects very specific versions of Juniper Networks Junos OS: 19.3R3-S2; 19.4R3-S3; 20.2 versions 20.2R2-S3 and later, prior to 20.2R3-S2; 20.3 versions 20.3R2 and later, prior to 20.3R3; 20.4 versions 20.4R2 and later, prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS 20.1 is not affected by this issue. This issue also affects	https://kb.juniper.net/JSA11218	O-JUN-JUNO-051121/4398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S3-EVO, 20.4R3-EVO; 21.1-EVO versions prior to 21.1R2-EVO; 21.2-EVO versions prior to 21.2R2-EVO. **CVE ID : CVE-2021-31353**		
Out-of-bounds Read	19-Oct-21	5.4	An Out Of Bounds (OOB) access vulnerability in the handling of responses by a Juniper Agile License (JAL) Client in Juniper Networks Junos OS and Junos OS Evolved, configured in Network Mode (to use Juniper Agile License Manager) may allow an attacker to cause a partial Denial of Service (DoS), or lead to remote code execution (RCE). The vulnerability exists in the packet parsing logic on the client that processes the response from the server using a custom protocol. An attacker with control of a JAL License Manager, or with access to the local broadcast domain, may be able to spoof a new JAL License Manager and/or craft a response to the Junos OS License Client, leading to exploitation of this vulnerability. This issue only affects Junos systems configured in Network Mode. Systems that are configured in Standalone	https://kb.juniper.net/JSA11219	O-JUN-JUNO-051121/4399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mode (the default mode of operation for all systems) are not vulnerable to this issue. This issue affects: Juniper Networks Junos OS: 19.2 versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: version 20.1R1-EVO and later versions, prior to 21.2R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2021-31354**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent cross-site scripting (XSS) vulnerability in the captive portal graphical user interface of Juniper Networks Junos OS may allow a remote authenticated user to inject web script or HTML and steal sensitive data and credentials from a web administration session, possibly tricking a follow-on administrative user to perform administrative actions on the device. This issue affects Juniper Networks Junos OS: All	https://kb.juniper.net/JSA11220	O-JUN-JUNO-051121/4400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, including the following supported releases: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D220; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R1-S1, 20.2R2; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31355**		
Improper Privilege Management	19-Oct-21	7.2	A local privilege escalation vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privileged user to cause the Juniper DHCP daemon (jdhcpd) process to crash, resulting in a Denial of Service (DoS), or execute arbitrary commands as root. Continued processing of malicious input will repeatedly crash the system and sustain the Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: All versions, including the following supported	https://kb.juniper.net/JSA11222	O-JUN-JUNO-051121/4401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			releases: 15.1 versions prior to 15.1R7-S10; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S3-EVO; All versions of 21.1-EVO. **CVE ID : CVE-2021-31359**		
Improper Input Validation	19-Oct-21	6.6	An improper privilege management vulnerability in the Juniper Networks Junos OS and Junos OS Evolved command-line interpreter (CLI) allows a low-privileged user to overwrite local files as root, possibly leading to a system integrity issue or Denial of Service (DoS). Depending on the files overwritten, exploitation of this vulnerability could lead to a sustained Denial of Service (DoS) condition, requiring manual user	https://kb.juniper.net/JSA11222	O-JUN-JUNO-051121/4402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			intervention to recover. This issue affects: Juniper Networks Junos OS: All versions, including the following supported releases: 15.1 versions prior to 15.1R7-S10; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S3-EVO; All versions of 21.1-EVO. **CVE ID : CVE-2021-31360**		
Improper Check for Unusual or Exceptional Conditions	19-Oct-21	5	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with Improper Handling of Exceptional Conditions in Juniper Networks Junos OS on QFX Series and PTX Series allows an unauthenticated network based attacker to cause increased FPC CPU	https://kb.juniper.net/JSA11223	O-JUN-JUNO-051121/4403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			utilization by sending specific IP packets which are being VXLAN encapsulated leading to a partial Denial of Service (DoS). Continued receipted of these specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX Series: All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS on PTX Series: All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S5; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31361**		
N/A	19-Oct-21	3.3	A Protection Mechanism Failure vulnerability in RPD (routing protocol daemon) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause established IS-IS adjacencies to go down by sending a spoofed hello PDU leading to a Denial of Service (DoS) condition. Continued receipted of these spoofed PDUs will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions	https://kb.juniper.net/JSA11224	O-JUN-JUNO-051121/4404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R2-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2021-31362**		
Loop with Unreachable Exit Condition ('Infinite Loop')	19-Oct-21	3.3	In an MPLS P2MP environment a Loop with Unreachable Exit Condition vulnerability in the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause high load on RPD which in turn may lead to routing protocol flaps. If a system with sensor-based-stats enabled receives a specific LDP FEC this can lead to the above condition. Continued receipted of such an LDP FEC will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 19.2 version 19.2R2 and later versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks	https://kb.juniper.net/JSA11225	O-JUN-JUNO-051121/4405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS versions prior to 19.2R2. Juniper Networks Junos OS Evolved All versions prior to 20.1R2-S3-EVO; 20.3 versions prior to 20.3R1-S2-EVO. **CVE ID : CVE-2021-31363**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4.3	An Improper Check for Unusual or Exceptional Conditions vulnerability combined with a Race Condition in the flow daemon (flowd) of Juniper Networks Junos OS on SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2 allows an unauthenticated network based attacker sending specific traffic to cause a crash of the flowd/srxpfe process, responsible for traffic forwarding in SRX, which will cause a Denial of Service (DoS). Continued receipt and processing of this specific traffic will create a sustained Denial of Service (DoS) condition. This issue can only occur when specific packets are trying to create the same session and logging for session-close is configured as a policy action. Affected platforms are: SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2. Not affected platforms are:	https://kb.juniper.net/JSA11226	O-JUN-JUNO-051121/4406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX4000 Series, SRX5000 Series with SPC3, and vSRX Series. This issue affects Juniper Networks Junos OS SRX300 Series, SRX500 Series, SRX1500, and SRX5000 Series with SPC2: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31364**		
Uncontrolled Resource Consumption	19-Oct-21	2.9	An Uncontrolled Resource Consumption vulnerability in Juniper Networks Junos OS on EX2300, EX3400 and EX4300 Series platforms allows an adjacent attacker sending a stream of layer 2 frames will trigger an Aggregated Ethernet (AE) interface to go down and thereby causing a Denial of Service (DoS). By continuously sending a stream of specific layer 2 frames an attacker will sustain the Denial of Service	https://kb.juniper.net/JSA11227	O-JUN-JUNO-051121/4407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition. This issue affects: Juniper Networks Junos OS EX4300 Series All versions prior to 15.1R7-S7; 16.1 versions prior to 16.1R7-S8; 17.1 versions prior to 17.1R2-S12; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2. Juniper Networks Junos OS EX3400 and EX4300-MP Series All versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S9, 18.4R3-S7; 19.1 versions prior to 19.1R2-S3, 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.3R2. Juniper Networks Junos OS EX2300 Series All versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31365**		
Unchecked Return Value	19-Oct-21	3.3	An Unchecked Return Value vulnerability in the authd (authentication daemon) of Juniper Networks Junos OS on MX Series configured for subscriber management / BBE allows an adjacent attacker to cause a crash by sending a specific username. This impacts authentication, authorization, and accounting (AAA) services on the MX devices and leads to a Denial of Service (DoS) condition. Continued receipted of these PPP login request will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks	https://kb.juniper.net/JSA11228	O-JUN-JUNO-051121/4408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. **CVE ID : CVE-2021-31366**		
Missing Release of Memory after Effective Lifetime	19-Oct-21	2.9	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows an adjacent attacker to cause a Denial of Service (DoS) by sending genuine BGP flowspec packets which cause an FPC heap memory leak. Once having run out of memory the FPC will crash and restart along with a core dump. Continued receipted of these packets will create a sustained Denial of Service	https://kb.juniper.net/JSA11229	O-JUN-JUNO-051121/4409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos Evolved is not affected. **CVE ID : CVE-2021-31367**		
Uncontrolled Resource Consumption	19-Oct-21	7.8	An Uncontrolled Resource Consumption vulnerability in the kernel of Juniper Networks JUNOS OS allows an unauthenticated network based attacker to cause 100% CPU load and the device to become unresponsive by sending a flood of traffic to the out-of-band management ethernet port. Continued receipted of a flood will create a sustained Denial of Service (DoS) condition. Once the flood subsides the system will recover by itself. An indication that the system is affected by this issue would be that kernel and netisr process are shown to be	https://kb.juniper.net/JSA11230	O-JUN-JUNO-051121/4410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using a lot of CPU cycles like in the following example output: user@host> show system processes extensive ... PID USERNAME PRI NICE SIZE RES STATE C TIME WCPU COMMAND 16 root -72 - 0K 304K WAIT 1 839:40 88.96% intr{swi1: netisr 0} 0 root 97 - 0K 160K RUN 1 732:43 87.99% kernel{bcm560xgmac0 que} This issue affects Juniper Networks JUNOS OS on EX2300 Series, EX3400 Series, and ACX710: All versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S9; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. **CVE ID : CVE-2021-31368**		
Allocation of Resources Without Limits or Throttling	19-Oct-21	4.3	On MX Series platforms with MS-MPC/MS-MIC, an Allocation of Resources Without Limits or Throttling vulnerability in Juniper	https://kb.juniper.net/JSA11231	O-JUN-JUNO-051121/4411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS allows an unauthenticated network attacker to cause a partial Denial of Service (DoS) with a high rate of specific traffic. If a Class of Service (CoS) rule is attached to the service-set and a high rate of specific traffic is processed by this service-set, for some of the other traffic which has services applied and is being processed by this MS-MPC/MS-MIC drops will be observed. Continued receipted of this high rate of specific traffic will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series with MS-MPC/MS-MIC: All versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31369**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Oct-21	3.3	An Incomplete List of Disallowed Inputs vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an adjacent unauthenticated attacker which sends a high rate of specific multicast traffic to cause control traffic received from the network to be dropped. This will impact control protocols (including but not limited to routing-protocols) and lead to a Denial of Service (DoS). Continued receipt of this specific multicast traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 and EX4600 Series: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to	https://kb.juniper.net/JSA11232	O-JUN-JUNO-051121/4412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2021-31370**		
N/A	19-Oct-21	5	Juniper Networks Junos OS uses the 128.0.0.0/2 subnet for internal communications between the RE and PFEs. It was discovered that packets utilizing these IP addresses may egress an QFX5110 switch, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet, leading to an information exposure vulnerability. This issue affects: Juniper Networks Junos OS on QFX5110 Series: All versions prior to 17.3R3-S12; 18.1 versions prior to 18.1R3-S13; 18.3 versions prior to 18.3R3-S5; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2; **CVE ID : CVE-2021-31371**	https://kb.juniper.net/JSA11236	O-JUN-JUNO-051121/4413
Improper	19-Oct-21	9	An Improper Input	https://kb.ju	O-JUN-JUNO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Validation vulnerability in J-Web of Juniper Networks Junos OS allows a locally authenticated J-Web attacker to escalate their privileges to root over the target device. This issue affects: Juniper Networks Junos OS All versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2, 21.1R3; 21.2 versions prior to 21.2R1-S1, 21.2R2; **CVE ID : CVE-2021-31372**	niper.net/JSA11237	051121/4414
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-21	3.5	A persistent Cross-Site Scripting (XSS) vulnerability in Juniper Networks Junos OS on SRX Series, J-Web interface may allow a remote authenticated user to inject persistent and malicious scripts. An attacker can exploit this vulnerability to steal sensitive data and credentials from a web administration session, or hijack another user's active session to perform	https://kb.juniper.net/JSA11238	O-JUN-JUNO-051121/4415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrative actions. This issue affects: Juniper Networks Junos OS on SRX Series: 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3. **CVE ID : CVE-2021-31373**		
N/A	19-Oct-21	5	On Juniper Networks Junos OS and Junos OS Evolved devices processing a specially crafted BGP UPDATE or KEEPALIVE message can lead to a routing process daemon (RPD) crash and restart, causing a Denial of Service (DoS). Continued receipt and processing of this message will create a sustained Denial of Service (DoS) condition. This issue affects both IBGP and EBGP deployments over IPv4 or IPv6. This issue affects: Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-	https://kb.juniper.net/JSA11239	O-JUN-JUNO-051121/4416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R1-S4, 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS Evolved: 20.3 versions prior to 20.3R2-EVO. **CVE ID : CVE-2021-31374**		
Improper Input Validation	19-Oct-21	5	An Improper Input Validation vulnerability in routing process daemon (RPD) of Juniper Networks Junos OS devices configured with BGP origin validation using Resource Public Key Infrastructure (RPKI), allows an attacker to send a specific BGP update which may cause RPKI policy-checks to be bypassed. This, in turn, may allow a spoofed advertisement to be accepted or propagated. This issue affects: Juniper Networks Junos OS 12.3	https://kb.juniper.net/JSA11240	O-JUN-JUNO-051121/4417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 12.3R12-S18; 15.1 versions prior to 15.1R7-S9; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2021-31375**		
Improper Input Validation	19-Oct-21	5	An Improper Input Validation vulnerability in Packet Forwarding Engine manager (FXPC) process of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending specific DHCPv6 packets to the device and crashing the FXPC service. Continued receipt and processing of this specific packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms in ACX Series: ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096 devices. Other ACX platforms are not affected from this issue. This issue	https://kb.juniper.net/JSA11241	O-JUN-JUNO-051121/4418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects Juniper Networks Junos OS on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096: 18.4 version 18.4R3-S7 and later versions prior to 18.4R3-S8. This issue does not affect: Juniper Networks Junos OS 18.4 versions prior to 18.4R3-S7 on ACX500, ACX1000, ACX1100, ACX2100, ACX2200, ACX4000, ACX5048, ACX5096. **CVE ID : CVE-2021-31376**		
Incorrect Permission Assignment for Critical Resource	19-Oct-21	2.1	An Incorrect Permission Assignment for Critical Resource vulnerability of a certain file in the filesystem of Junos OS allows a local authenticated attacker to cause routing process daemon (RPD) to crash and restart, causing a Denial of Service (DoS). Repeated actions by the attacker will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to	https://kb.juniper.net/JSA11242	O-JUN-JUNO-051121/4419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4R2-S8, 18.4R3-S7; 19.1 versions prior to 19.1R2-S3, 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R1-S1, 20.4R2. **CVE ID : CVE-2021-31377**		
Missing Release of Resource after Effective Lifetime	19-Oct-21	4.3	In broadband environments, including but not limited to Enhanced Subscriber Management, (CHAP, PPP, DHCP, etc.), on Juniper Networks Junos OS devices where RADIUS servers are configured for managing subscriber access and a subscriber is logged in and then requests to logout, the subscriber may be forced into a "Terminating" state by an attacker who is able to send spoofed messages appearing to originate from trusted RADIUS server(s) destined to the device in response to the subscriber's request. These spoofed messages cause the Junos OS General Authentication Service (authd) daemon to force the broadband subscriber into this	https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/topic-map/general-authentication-service-events-tracing.html, https://kb.juniper.net/JSA11246	O-JUN-JUNO-051121/4420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"Terminating" state which the subscriber will not recover from thereby causing a Denial of Service (DoS) to the endpoint device. Once in the "Terminating" state, the endpoint subscriber will no longer be able to access the network. Restarting the authd daemon on the Junos OS device will temporarily clear the subscribers out of the "Terminating" state. As long as the attacker continues to send these spoofed packets and subscribers request to be logged out, the subscribers will be returned to the "Terminating" state thereby creating a persistent Denial of Service to the subscriber. An indicator of compromise may be seen by displaying the output of "show subscribers summary". The presence of subscribers in the "Terminating" state may indicate the issue is occurring. This issue affects: Juniper Networks Junos OS 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S9; 19.1 versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R1-S4, 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. This issue does not affect: Juniper Networks Junos OS 12.3 version 12.3R1 and later versions; 15.1 version 15.1R1 and later versions. **CVE ID : CVE-2021-31378**		
N/A	19-Oct-21	4.3	An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets. Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition. This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. An	https://kb.juniper.net/JSA11247, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/map-e-configuring.html	O-JUN-JUNO-051121/4421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			indicator of compromise is the output: FPC ["FPC ID" # e.g. "0"] PFE #{PFE ID # e.g. "1"] : Fabric Disabled Example: FPC 0 PFE #1 : Fabric Disabled when using the command: show chassis fabric fpcs An example of a healthy result of the command use would be: user@device-re1> show chassis fabric fpcs Fabric management FPC state: FPC 0 PFE #0 Plane 0: Plane enabled Plane 1: Plane enabled Plane 2: Plane enabled Plane 3: Plane enabled Plane 4: Plane enabled Plane 5: Plane enabled Plane 6: Plane enabled Plane 7: Plane enabled This issue affects: Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards. 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. **CVE ID : CVE-2021-31379**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	6.8	On PTX1000 System, PTX10002-60C System, after upgrading to an affected release, a Race Condition vulnerability between the chassis daemon (chassisd) and firewall process (dfwd) of Juniper Networks Junos OS, may update the device's interfaces with incorrect firewall filters. This issue only occurs when upgrading the device to an affected version of Junos OS. Interfaces intended to have protections may have no protections assigned to them. Interfaces with one type of protection pattern may have alternate protections assigned to them. Interfaces intended to have no protections may have protections assigned to them. These firewall rule misassignments may allow genuine traffic intended to be stopped at the interface to propagate further, potentially causing disruptions in services by propagating unwanted traffic. An attacker may be able to take advantage of	https://kb.juniper.net/JSA11250, https://kb.juniper.net/KB10956	O-JUN-JUNO-051121/4422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these misassignments. This issue affects Juniper Networks Junos OS on PTX1000 System: 17.2 versions 17.2R1 and later versions prior to 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R1-S1, 20.4R2. This issue does not affect Juniper Networks Junos OS prior to version 17.2R1 on PTX1000 System. This issue affects Juniper Networks Junos OS on PTX10002-60C System: 18.2 versions 18.2R1 and later versions prior to 18.4 versions prior to 18.4R3-S9; 19.1 versions later than 19.1R1 prior to 19.4 versions prior to 19.4R2-S5, 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions 20.4R1 and later versions prior to 21.1 versions prior to 21.1R2; 21.2 versions 21.2R1 and later versions prior to 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS prior to version 18.2R1 on PTX10002-60C System. This issue impacts all filter families (inet, inet6, etc.) and all loopback filters. It does not rely upon the location where a filter is set, impacting both logical and physical interfaces. **CVE ID : CVE-2021-31382**		
Out-of-bounds Write	19-Oct-21	4.3	In Point to MultiPoint (P2MP) scenarios within established sessions between network or adjacent neighbors the improper use of a source to destination copy write operation combined with a Stack-based Buffer Overflow on certain specific packets processed by the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved sent by a remote unauthenticated network attacker causes the RPD to crash causing a Denial of Service (DoS). Continued receipt and processing of these packets	https://kb.juniper.net/JSA11251	O-JUN-JUNO-051121/4423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. Juniper Networks Junos OS Evolved 20.1 versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R3-EVO; 20.3 versions prior to 20.3R2-EVO. **CVE ID : CVE-2021-31383**		
Missing Authorization	19-Oct-21	7.5	Due to a Missing Authorization weakness and Insufficient Granularity of Access Control in a specific device configuration, a vulnerability exists in Juniper Networks Junos OS on SRX Series whereby an attacker who attempts to access J-Web administrative interfaces can successfully do so from any device interface regardless of the web-management configuration and filter rules which may otherwise	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252	O-JUN-JUNO-051121/4424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protect access to J-Web. This issue affects: Juniper Networks Junos OS SRX Series 20.4 version 20.4R1 and later versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2021-31384**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-21	8.5	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in J-Web of Juniper Networks Junos OS allows any low-privileged authenticated attacker to elevate their privileges to root. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S19; 15.1 versions prior to 15.1R7-S10; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1,	https://kb.juniper.net/JSA11253	O-JUN-JUNO-051121/4425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.1R2. **CVE ID : CVE-2021-31385**		
N/A	19-Oct-21	2.6	A Protection Mechanism Failure vulnerability in the J-Web HTTP service of Juniper Networks Junos OS allows a remote unauthenticated attacker to perform Person-in-the-Middle (PitM) attacks against the device. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S20; 15.1 versions prior to 15.1R7-S11; 18.3 versions prior to 18.3R3-S6; 18.4 versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. **CVE ID : CVE-2021-31386**	https://kb.juniper.net/JSA11254	O-JUN-JUNO-051121/4426
junos_os_evolved					
Improper Handling of Exceptional Conditions	19-Oct-21	6.4	A vulnerability in the processing of TCP MD5 authentication in Juniper Networks Junos OS Evolved may allow a BGP or LDP session configured with MD5 authentication to succeed,	https://kb.juniper.net/JSA11211	O-JUN-JUNO-051121/4427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			even if the peer does not have TCP MD5 authentication enabled. This could lead to untrusted or unauthorized sessions being established, resulting in an impact on confidentiality or stability of the network. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.3R2-S1-EVO; 20.4 versions prior to 20.4R2-EVO; 21.1 versions prior to 21.1R2-EVO. Juniper Networks Junos OS is not affected by this issue. **CVE ID : CVE-2021-0297**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Oct-21	4	A Race Condition in the 'show chassis pic' command in Juniper Networks Junos OS Evolved may allow an attacker to crash the port interface concentrator daemon (picd) process on the FPC, if the command is executed coincident with other system events outside the attacker's control, leading to a Denial of Service (DoS) condition. Continued execution of the CLI command, under precise conditions, could create a sustained Denial of Service (DoS) condition. This issue affects all Juniper Networks Junos OS Evolved versions prior to 20.1R2-EVO on PTX10003 and PTX10008	https://kb.juniper.net/JSA11212	O-JUN-JUNO-051121/4428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			platforms. Junos OS is not affected by this vulnerability. **CVE ID : CVE-2021-0298**		
Improper Privilege Management	19-Oct-21	9	An Improper Privilege Management vulnerability in the gRPC framework, used by the Juniper Extension Toolkit (JET) API on Juniper Networks Junos OS and Junos OS Evolved, allows a network-based, low-privileged authenticated attacker to perform operations as root, leading to complete compromise of the targeted system. The issue is caused by the JET service daemon (jsd) process authenticating the user, then passing configuration operations directly to the management daemon (mgd) process, which runs as root. This issue affects Juniper Networks Junos OS: 18.4 versions prior to 18.4R1-S8, 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R2-S3, 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. This issue does	https://kb.juniper.net/JSA11215	O-JUN-JUNO-051121/4429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not affect Juniper Networks Junos OS versions prior to 18.4R1. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO. **CVE ID : CVE-2021-31350**		
Improper Handling of Exceptional Conditions	19-Oct-21	5	An Improper Handling of Exceptional Conditions vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an attacker to inject a specific BGP update, causing the routing protocol daemon (RPD) to crash and restart, leading to a Denial of Service (DoS). Continued receipt and processing of the BGP update will create a sustained Denial of Service (DoS) condition. This issue affects very specific versions of Juniper Networks Junos OS: 19.3R3-S2; 19.4R3-S3; 20.2 versions 20.2R2-S3 and later, prior to 20.2R3-S2; 20.3 versions 20.3R2 and later, prior to 20.3R3; 20.4 versions 20.4R2 and later, prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS 20.1 is not affected by this issue. This issue also affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S3-EVO, 20.4R3-EVO; 21.1-EVO versions	https://kb.juniper.net/JSA11218	O-JUN-JUNO-051121/4430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.1R2-EVO; 21.2-EVO versions prior to 21.2R2-EVO. **CVE ID : CVE-2021-31353**		
Out-of-bounds Read	19-Oct-21	5.4	An Out Of Bounds (OOB) access vulnerability in the handling of responses by a Juniper Agile License (JAL) Client in Juniper Networks Junos OS and Junos OS Evolved, configured in Network Mode (to use Juniper Agile License Manager) may allow an attacker to cause a partial Denial of Service (DoS), or lead to remote code execution (RCE). The vulnerability exists in the packet parsing logic on the client that processes the response from the server using a custom protocol. An attacker with control of a JAL License Manager, or with access to the local broadcast domain, may be able to spoof a new JAL License Manager and/or craft a response to the Junos OS License Client, leading to exploitation of this vulnerability. This issue only affects Junos systems configured in Network Mode. Systems that are configured in Standalone Mode (the default mode of operation for all systems) are not vulnerable to this issue. This issue affects:	https://kb.juniper.net/JSA11219	O-JUN-JUNO-051121/4431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS: 19.2 versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. Juniper Networks Junos OS Evolved: version 20.1R1-EVO and later versions, prior to 21.2R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. **CVE ID : CVE-2021-31354**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Oct-21	7.2	A command injection vulnerability in command processing on Juniper Networks Junos OS Evolved allows an attacker with authenticated CLI access to be able to bypass configured access protections to execute arbitrary shell commands within the context of the current user. The vulnerability allows an attacker to bypass command authorization restrictions assigned to their specific user account and execute commands that are available to the privilege level for which the user is assigned. For example, a user that is in the super-user login class,	https://kb.juniper.net/JSA11221	O-JUN-JUNO-051121/4432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			but restricted to executing specific CLI commands could exploit the vulnerability to execute any other command available to an unrestricted admin user. This vulnerability does not increase the privilege level of the user, but rather bypasses any CLI command restrictions by allowing full access to the shell. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S1-EVO; All versions of 21.1-EVO and 21.2-EVO. **CVE ID : CVE-2021-31356**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Oct-21	7.2	A command injection vulnerability in tcpdump command processing on Juniper Networks Junos OS Evolved allows an attacker with authenticated CLI access to be able to bypass configured access protections to execute arbitrary shell commands within the context of the current user. The vulnerability allows an attacker to bypass command authorization restrictions assigned to their specific user account and execute commands that are available to the privilege level for which the user is assigned. For example, a user that is in the super-user login class,	https://kb.juniper.net/JSA11221	O-JUN-JUNO-051121/4433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			but restricted to executing specific CLI commands could exploit the vulnerability to execute any other command available to an unrestricted admin user. This vulnerability does not increase the privilege level of the user, but rather bypasses any CLI command restrictions by allowing full access to the shell. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.3R2-S1-EVO; 20.4 versions prior to 20.4R2-S2-EVO; 21.1 versions prior to 21.1R2-EVO; 21.2 versions prior to 21.2R1-S1-EVO, 21.2R2-EVO. **CVE ID : CVE-2021-31357**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Oct-21	7.2	A command injection vulnerability in sftp command processing on Juniper Networks Junos OS Evolved allows an attacker with authenticated CLI access to be able to bypass configured access protections to execute arbitrary shell commands within the context of the current user. The vulnerability allows an attacker to bypass command authorization restrictions assigned to their specific user account and execute commands that are available to the privilege level for	https://kb.juniper.net/JSA11221	O-JUN-JUNO-051121/4434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which the user is assigned. For example, a user that is in the super-user login class, but restricted to executing specific CLI commands could exploit the vulnerability to execute any other command available to an unrestricted admin user. This vulnerability does not increase the privilege level of the user, but rather bypasses any CLI command restrictions by allowing full access to the shell. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S2-EVO; 21.1 versions prior to 21.1R2-EVO; 21.2 versions prior to 21.2R1-S1-EVO, 21.2R2-EVO. **CVE ID : CVE-2021-31358**		
Improper Privilege Management	19-Oct-21	7.2	A local privilege escalation vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privileged user to cause the Juniper DHCP daemon (jdhcpd) process to crash, resulting in a Denial of Service (DoS), or execute arbitrary commands as root. Continued processing of malicious input will repeatedly crash the system and sustain the Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: All	https://kb.juniper.net/JSA11222	O-JUN-JUNO-051121/4435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions, including the following supported releases: 15.1 versions prior to 15.1R7-S10; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S3-EVO; All versions of 21.1-EVO. **CVE ID : CVE-2021-31359**		
Improper Input Validation	19-Oct-21	6.6	An improper privilege management vulnerability in the Juniper Networks Junos OS and Junos OS Evolved command-line interpreter (CLI) allows a low-privileged user to overwrite local files as root, possibly leading to a system integrity issue or Denial of Service (DoS). Depending on the files overwritten, exploitation of this vulnerability could lead to a sustained Denial of	https://kb.juniper.net/JSA11222	O-JUN-JUNO-051121/4436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) condition, requiring manual user intervention to recover. This issue affects: Juniper Networks Junos OS: All versions, including the following supported releases: 15.1 versions prior to 15.1R7-S10; 17.4 versions prior to 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S3-EVO; All versions of 21.1-EVO. **CVE ID : CVE-2021-31360**		
N/A	19-Oct-21	3.3	A Protection Mechanism Failure vulnerability in RPD (routing protocol daemon) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cause established IS-IS adjacencies to go down by	https://kb.juniper.net/JSA11224	O-JUN-JUNO-051121/4437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending a spoofed hello PDU leading to a Denial of Service (DoS) condition. Continued receipted of these spoofed PDUs will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS All versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R2-EVO; 21.1 versions prior to 21.1R2-EVO. **CVE ID : CVE-2021-31362**		
Loop with Unreachable Exit Condition ('Infinite Loop')	19-Oct-21	3.3	In an MPLS P2MP environment a Loop with Unreachable Exit Condition vulnerability in the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause high load on RPD which in turn may lead to routing protocol flaps. If a system with	https://kb.juniper.net/JSA11225	O-JUN-JUNO-051121/4438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensor-based-stats enabled receives a specific LDP FEC this can lead to the above condition. Continued receipted of such an LDP FEC will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 19.2 version 19.2R2 and later versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R2. Juniper Networks Junos OS Evolved All versions prior to 20.1R2-S3-EVO; 20.3 versions prior to 20.3R1-S2-EVO. **CVE ID : CVE-2021-31363**		
N/A	19-Oct-21	5	On Juniper Networks Junos OS and Junos OS Evolved devices processing a specially crafted BGP UPDATE or KEEPALIVE message can lead to a routing process daemon (RPD) crash and restart, causing a Denial of Service (DoS). Continued receipt and processing of this message	https://kb.juniper.net/JSA11239	O-JUN-JUNO-051121/4439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			will create a sustained Denial of Service (DoS) condition. This issue affects both IBGP and EBGP deployments over IPv4 or IPv6. This issue affects: Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R1-S4, 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS Evolved: 20.3 versions prior to 20.3R2-EVO. **CVE ID : CVE-2021-31374**		
Out-of-bounds Write	19-Oct-21	4.3	In Point to MultiPoint (P2MP) scenarios within established sessions between network or adjacent neighbors the improper use of a source to destination copy write	https://kb.juniper.net/JSA11251	O-JUN-JUNO-051121/4440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operation combined with a Stack-based Buffer Overflow on certain specific packets processed by the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved sent by a remote unauthenticated network attacker causes the RPD to crash causing a Denial of Service (DoS). Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 19.2R1. Juniper Networks Junos OS Evolved 20.1 versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R3-EVO; 20.3 versions prior to 20.3R2-EVO. **CVE ID : CVE-2021-31383**		
Linux					
linux_kernel					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-21	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.28. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: This vulnerability does not apply to Windows systems. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35538**	https://www.oracle.com/security-alerts/cpuoct2021.html	O-LIN-LINU-051121/4441
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-21	4.3	IBM QRadar Advisor 2.5 through 2.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 209566. **CVE ID : CVE-2021-38896**	https://www.ibm.com/support/pages/node/6506461, https://exchange.xforce.ibmcloud.com/vulnerabilities/209566	O-LIN-LINU-051121/4442
Out-of-	21-Oct-21	4.6	dp_link_settings_write in	https://git.k	O-LIN-LINU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			drivers/gpu/drm/amd/display/amdgpu_dm/amdgpu_dm_debugfs.c in the Linux kernel through 5.14.14 allows a heap-based buffer overflow by an attacker who can write a string to the AMD GPU display drivers debug filesystem. There are no checks on size within parse_write_buffer_into_params when it uses the size of copy_from_user to copy a userspace buffer into a 40-byte heap buffer. **CVE ID : CVE-2021-42327**	ernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/log/drivers/gpu/drm/amd/display/amdgpu_dm/amdgpu_dm_debugfs.c, https://www.mail-archive.com/amd-gfx@lists.freedesktop.org/msg69080.html	051121/4443
Out-of-bounds Write	20-Oct-21	4.6	The firewire subsystem in the Linux kernel through 5.14.13 has a buffer overflow related to drivers/media/firewire/firedtv-avc.c and drivers/media/firewire/firedtv-ci.c, because avc_ca_pmt mishandles bounds checking. **CVE ID : CVE-2021-42739**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=35d2969ea3c7d32aee78066b1f3cf61a0d935a4e, https://seclists.org/oss-sec/2021/q2/46	O-LIN-LINU-051121/4444
Microsoft					
surface_pro_3_firmware					
Incorrect Authorization	20-Oct-21	3.6	Microsoft Surface Pro 3 Security Feature Bypass Vulnerability	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-SURF-051121/4445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-42299	guidance/advisory/CVE-2021-42299	
windows					
Incorrect Default Permissions	21-Oct-21	4.6	An incorrect permission assignment vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to load a DLL with escalated privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-42011**	https://success.trendmicro.com/solution/000289229	O-MIC-WIND-051121/4446
Uncontrolled Search Path Element	21-Oct-21	4.6	An uncontrolled search path element vulnerabilities in Trend Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar but not identical to CVE-2021-42103. **CVE ID : CVE-2021-42101**	https://success.trendmicro.com/solution/000289229	O-MIC-WIND-051121/4447
Uncontrolled Search Path Element	21-Oct-21	4.6	An uncontrolled search path element vulnerabilities in Trend Micro Apex One and Apex One as a Service agents could allow a local attacker	https://success.trendmicro.com/solution/000289229	O-MIC-WIND-051121/4448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to escalate privileges on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-42102**		
Uncontrolled Search Path Element	21-Oct-21	4.6	An uncontrolled search path element vulnerabilities in Trend Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar but not identical to CVE-2021-42101. **CVE ID : CVE-2021-42103**	https://success.trendmicro.com/solution/000289229	O-MIC-WIND-051121/4449
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	O-MIC-WIND-051121/4450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not identical to CVE-2021-42105, 42106 and 42107. **CVE ID : CVE-2021-42104**		
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42106 and 42107. **CVE ID : CVE-2021-42105**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	O-MIC-WIND-051121/4451
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42105 and 42107.	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	O-MIC-WIND-051121/4452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-42106		
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in Trend Micro Apex One, Apex One as a Service, Worry-Free Business Security 10.0 SP1 and Worry-Free Business Security Services could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-42104, 42105 and 42106. **CVE ID : CVE-2021-42107**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	O-MIC-WIND-051121/4453
Improper Privilege Management	21-Oct-21	4.6	Unnecessary privilege vulnerabilities in the Web Console of Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-42108**	https://success.trendmicro.com/solution/000289230, https://success.trendmicro.com/solution/000289229	O-MIC-WIND-051121/4454
NULL Pointer Dereference	21-Oct-21	5	A null pointer vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 could	https://success.trendmicro.com/solution/000289	O-MIC-WIND-051121/4455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to crash the CGI program on affected installations. **CVE ID : CVE-2021-23139**	30, https://success.trendmicro.com/solution/000289229	
Uncontrolled Search Path Element	22-Oct-21	7.2	The Harmony Browse and the SandBlast Agent for Browsers installers must have admin privileges to execute some steps during the installation. Because the MS Installer allows regular users to repair their installation, an attacker running an installer before 90.08.7405 can start the installation repair and place a specially crafted binary in the repair folder, which runs with the admin privileges. **CVE ID : CVE-2021-30359**	https://supportcontent.checkpoint.com/solutions?id=sk175968	O-MIC-WIND-051121/4456
Netapp					
clustered_data_ontap					
Exposure of Resource to Wrong Sphere	19-Oct-21	2.1	Clustered Data ONTAP versions 9.x prior to 9.5P18, 9.6P16, 9.7P16, 9.8P7 and 9.9.1P2 are susceptible to a vulnerability which could allow an authenticated privileged local attacker to arbitrarily modify Compliance-mode WORM data prior to the end of the retention period. **CVE ID : CVE-2021-27001**	https://security.netapp.com/advisory/ntap-20211018-0001	O-NET-CLUS-051121/4457
onepeloton					
ttr01_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Calculation of Buffer Size	25-Oct-21	5	Incorrect calculation of buffer size vulnerability in Peleton TTR01 up to and including PTV55G allows a remote attacker to trigger a Denial of Service attack through the GymKit daemon process by exploiting a heap overflow in the network server handling the Apple GymKit communication. This can lead to an Apple MFI device not being able to authenticate with the Peleton Bike **CVE ID : CVE-2021-40526**	https://twitter.com/ROPsicle/status/1438216078103044107?s=20	O-ONE-TTR0-051121/4458
openpowerfoundation					
skiboot					
Incorrect Conversion between Numeric Types	22-Oct-21	7.5	An issue was discovered in OpenPOWER 2.6 firmware. unpack_timestamp() calls le32_to_cpu() for endian conversion of a uint16_t "year" value, resulting in a type mismatch that can truncate a higher integer value to a smaller one, and bypass a timestamp check. The fix is to use the right endian conversion function. **CVE ID : CVE-2021-36357**	https://github.com/open-power/skiboot/commit/5be38b672c1410e2f10acd3ad2eecfdc81d5daf7	O-OPE-SKIB-051121/4459
Oracle					
solaris					
N/A	20-Oct-21	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is	https://www.oracle.com/security-alerts/cpuoct2021.html	O-ORA-SOLA-051121/4460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected is Prior to 6.1.28. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: This vulnerability does not apply to Windows systems. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-35538**		
N/A	20-Oct-21	4.9	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause	https://www.oracle.com/security-alerts/cpuoct2021.html	O-ORA-SOLA-051121/4461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2021-35539**		
N/A	20-Oct-21	3.3	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L). **CVE ID : CVE-2021-35549**	https://www.oracle.com/security-alerts/cpuoct2021.html	O-ORA-SOLA-051121/4462
N/A	20-Oct-21	4.9	Vulnerability in the Oracle	https://ww	O-ORA-SOLA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Solaris product of Oracle Systems (component: Device drivers). The supported version that is affected is 11. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2021-35589**	w.oracle.com/security-alerts/cpuoct2021.html	051121/4463
Qualcomm					
apq8009w_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4465
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4466
apq8009_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4467
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of	https://www.qualcomm.	O-QUA-APQ8-051121/4468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4469
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4471
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4472
apq8017_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-APQ8-051121/4473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1917**	bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4474
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4475
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4476
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while	https://www.qualcomm.com/compan	O-QUA-APQ8-051121/4477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4478
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4479
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-APQ8-051121/4480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4481
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4482
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4483
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-APQ8-051121/4484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4485
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4486
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30310		
apq8037_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4488
apq8053_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4489
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4490
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in	https://www.qualcomm.com/company/product-	O-QUA-APQ8-051121/4491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4492
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4493
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption	https://www.qualcomm.com/company/product-	O-QUA-APQ8-051121/4494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4495
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4497
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4498
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4499
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30257		
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4501
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4502
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4503
Out-of-	20-Oct-21	7.2	Possible memory corruption	https://ww	O-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/4504
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4505
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4506
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4508
apq8064au_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4509
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4511
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4512
Buffer Copy without Checking Size of Input	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in	https://www.qualcomm.com/company/product-	O-QUA-APQ8-051121/4513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4514
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4515
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4517
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4518
apq8096au_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4519
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4521
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4522
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-APQ8-051121/4523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4524
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4525
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1985**		
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4527
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4528
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4530
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4531
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-APQ8-051121/4532
aqt1000_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in	https://www.qualcomm.com/company/product-	O-QUA-AQT1-051121/4533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4534
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4535
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-AQT1-051121/4536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	etins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4537
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4538
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1966		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4540
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4541
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4543
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4544
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-AQT1-051121/4545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4546
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4547
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4548
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-AQT1-051121/4549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4550
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4551
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30292**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4553
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4554
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AQT1-051121/4555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
ar8031_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4556
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4557
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4559
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4560
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-AR80-051121/4561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4562
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4564
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4565
ar8035_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**		
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4567
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4568
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-AR80-051121/4569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4570
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4571
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information	https://www.qualcomm.com/company/product-security/bull	O-QUA-AR80-051121/4572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4573
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4575
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR80-051121/4576
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-AR80-051121/4577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
ar9380_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR93-051121/4578
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR93-051121/4579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-AR93-051121/4580
csr6030_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSR6-051121/4581
csr8811_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-CSR8-051121/4582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSR8-051121/4583
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSR8-051121/4584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSR8-051121/4585
csra6620_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4586
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-CSRA-051121/4587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4588
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4589
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-CSRA-051121/4590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4591
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4593
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4594
Improper Restriction of Operations within the Bounds of a	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-CSRA-051121/4595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	etins/octobe r-2021-bulletin	
csra6640_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4596
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4597
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4599
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4600
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in	https://www.qualcomm.com/company/product-security/bull	O-QUA-CSRA-051121/4601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4602
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4604
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRA-051121/4605
csrb31024_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-CSRB-051121/4606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRB-051121/4607
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRB-051121/4608
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-CSRB-051121/4609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRB-051121/4610
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-CSRB-051121/4611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30310		
fsm10055_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4612
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4613
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4614
Exposure of	20-Oct-21	2.1	Improper validation of	https://ww	O-QUA-FSM1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/4615
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4616
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4618
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4619
fsm10056_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4621
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4622
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4624
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4625
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-FSM1-051121/4626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-FSM1-051121/4627
ipq4018_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ4-051121/4628
Improper Authenticatio	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames	https://www.qualcomm.	O-QUA-IPQ4-051121/4629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ4-051121/4630
ipq4019_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ4-051121/4631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ4-051121/4632
ipq4028_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ4-051121/4633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ4-051121/4634
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ4-051121/4635
ipq4029_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-IPQ4-051121/4636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ4-051121/4637
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ4-051121/4638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
ipq5010_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ5-051121/4639
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ5-051121/4640
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information	https://www.qualcomm.com/company/product-	O-QUA-IPQ5-051121/4641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ5-051121/4642
ipq5018_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ5-051121/4643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ5-051121/4644
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ5-051121/4645
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	O-QUA-IPQ5-051121/4646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	
ipq5028_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ5-051121/4647
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ5-051121/4648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ5-051121/4649
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ5-051121/4650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
ipq6000_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4651
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4652
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information	https://www.qualcomm.com/company/product-	O-QUA-IPQ6-051121/4653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4654
ipq6005_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4656
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4657
ipq6010_firmware					
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	O-QUA-IPQ6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/4658
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4659
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4661
ipq6018_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4663
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4664
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-IPQ6-051121/4665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
ipq6028_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4666
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4668
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ6-051121/4669
ipq8064_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check	https://www.qualcomm.	O-QUA-IPQ8-051121/4670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4671
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
ipq8065_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4673
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4674
ipq8068_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4675
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4676
ipq8069_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-IPQ8-051121/4677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4678
ipq8070a_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4680
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4681
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-051121/4682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	security/bulletins/october-2021-bulletin	
ipq8070_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4683
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4685
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4686
ipq8071a_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4687
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4688
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-IPQ8-051121/4689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4690
ipq8071_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4692
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4693
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ8-051121/4694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	etins/october-2021-bulletin	
ipq8072a_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4695
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4697
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4698
ipq8072_firmware					
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	O-QUA-IPQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/4699
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4700
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4702
ipq8074a_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4704
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4705
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-IPQ8-051121/4706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
ipq8074_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4707
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4709
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4710
ipq8076a_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check	https://www.qualcomm.	O-QUA-IPQ8-051121/4711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4712
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4714
ipq8076_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4716
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4717
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
ipq8078a_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4719
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4721
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4722
ipq8078_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-051121/4723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4724
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4726
ipq8173_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4727
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of	https://www.qualcomm.	O-QUA-IPQ8-051121/4728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4729
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
ipq8174_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4731
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30288		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4733
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-IPQ8-051121/4734
mdm8207_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-MDM8-051121/4735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	r-2021-bulletin	
mdm9150_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4736
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4737
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-MDM9-051121/4738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4739
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4741
mdm9206_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4742
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4743
Out-of-	20-Oct-21	4.6	Possible stack buffer	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	MDM9-051121/4744
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4745
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
mdm9207_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4747
mdm9230_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4748
mdm9250_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4750
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4751
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-MDM9-051121/4752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	bulletin	
mdm9330_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4753
mdm9607_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4754
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-MDM9-051121/4755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4756
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4757
mdm9626_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while	https://www.qualcomm.com/compan	O-QUA-MDM9-051121/4758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4759
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4760
mdm9628_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4761
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4762
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4764
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4765
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4766
mdm9630_firmware					
Out-of-	20-Oct-21	7.2	Possible memory corruption	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	MDM9-051121/4767
mdm9640_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4768
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4769
mdm9650_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4770
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4771
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4773
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4774
mdm9655_firmware					
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MDM9-051121/4775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
msm8108_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4776
msm8208_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4777
msm8209_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-MSM8-051121/4778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	r-2021-bulletin	
msm8608_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4779
msm8909w_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4780
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4782
msm8917_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4783
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4784
Integer Overflow or	20-Oct-21	7.2	Possible integer overflow due to improper check of	https://www.qualcomm.	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	com/company/product-security/bulletins/october-2021-bulletin	051121/4785
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4786
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4787
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-MSM8-051121/4788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4789
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4790
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4791
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-MSM8-051121/4792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4793
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4794
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4795
msm8920_firmware					
Out-of-	20-Oct-21	7.2	Possible memory corruption	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	MSM8-051121/4796
msm8937_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4797
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4798
msm8940_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://www.qualcomm.com/compan	O-QUA-MSM8-051121/4799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
msm8953_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4800
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4801
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4803
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4804
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4806
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4807
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4809
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4810
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4811
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4813
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4814
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4815
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
msm8976sg_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4817
msm8976_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4818
msm8996au_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-MSM8-051121/4819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4820
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4821
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4823
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4824
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-MSM8-051121/4825

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4826
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4827
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4829
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4830
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-MSM8-051121/4831
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-MSM8-051121/4832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	security/bulletins/october-2021-bulletin	
pm8937_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-PM89-051121/4833
pmp8074_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-PMP8-051121/4834
Out-of-	20-Oct-21	7.2	Possible stack overflow due	https://ww	O-QUA-PMP8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/4835
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-PMP8-051121/4836
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-PMP8-051121/4837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qca1023_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA1-051121/4838
qca1062_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA1-051121/4839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA1-051121/4840
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA1-051121/4841
qca1064_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE	https://www.qualcomm.com/compan	O-QUA-QCA1-051121/4842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA1-051121/4843
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA1-051121/4844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
qca10901_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA1-051121/4845
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA1-051121/4846
qca1990_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA1-051121/4847
qca2062_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4848
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4850
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4851
qca2064_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA2-051121/4852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4853
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30302**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4855
qca2065_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4856
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4858
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4859
qca2066_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA2-051121/4860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4861
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30302**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA2-051121/4863
qca4010_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA4-051121/4864
qca4020_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA4-051121/4865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA4-051121/4866
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA4-051121/4867
Improper	20-Oct-21	5	Possible buffer overflow due	https://ww	O-QUA-QCA4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/4868
qca4024_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA4-051121/4869
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA4-051121/4870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA4-051121/4871
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA4-051121/4872
qca4531_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA4-051121/4873
qca6174a_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4874
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4875
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while	https://www.qualcomm.com/compan	O-QUA-QCA6-051121/4876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4877
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4878
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while	https://www.qualcomm.com/compan	O-QUA-QCA6-051121/4879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4880
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4881
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/4882
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4883
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4884
Improper Restriction of	20-Oct-21	7.2	Possible out of bound memory access due to	https://www.qualcomm.	O-QUA-QCA6-051121/4885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	com/company/product-security/bulletins/october-2021-bulletin	
qca6174_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4886
qca6175a_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4888
qca6310_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4889
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4890
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://www.qualcomm.com/compan	O-QUA-QCA6-051121/4891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4892
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4894
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4895
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4896
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-051121/4897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4898
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4899
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30292**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4901
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4902
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4904
qca6320_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4905
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4907
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4908
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4910
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4911
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4913
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4914
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4915
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30297**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4917
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4918
qca6330_firmware					
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/4919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	bulletin	
qca6335_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4920
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4921
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/4922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4923
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4924
Buffer Copy without	20-Oct-21	7.2	Possible buffer overflow due to improper handling of	https://www.qualcomm.	O-QUA-QCA6-051121/4925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	com/company/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4926
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4927
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30258		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4929
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4930
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4931
Buffer Copy	20-Oct-21	3.6	Possible out of bound read	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/4932
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4933
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
qca6390_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4935
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4936
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1932		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4938
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4939
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4940
Buffer Copy without Checking Size of Input	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in	https://www.qualcomm.com/company/product-	O-QUA-QCA6-051121/4941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4942
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4943
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/4944
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4945
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4946
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length	https://www.qualcomm.	O-QUA-QCA6-051121/4947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4948
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4949
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4950
Out-of-	20-Oct-21	7.2	Possible stack overflow due to improper length check of	https://www.qualcomm.	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	com/company/product-security/bulletins/october-2021-bulletin	051121/4951
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4952
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4953
Buffer Copy without Checking Size of Input	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR	https://www.qualcomm.com/company/product-	O-QUA-QCA6-051121/4954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4955
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4956
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qca6391_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4958
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4959
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1936**		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4961
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4962
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4963
Out-of-	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check	https://www.qualcomm.	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	com/company/product-security/bulletins/october-2021-bulletin	051121/4964
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4965
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1969		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4967
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4968
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-051121/4969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4970
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4971
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4972
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP	https://www.qualcomm.com/compan	O-QUA-QCA6-051121/4973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4974
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4975
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-051121/4976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4977
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4978
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30302		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4980
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4981
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4982
Improper Restriction of Operations within the Bounds of a	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/4983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	etins/october-2021-bulletin	
qca6420_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4984
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4985
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4987
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4988
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4990
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4991
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4993
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4994
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/4995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4996
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4997
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/4998
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in	https://www.qualcomm.com/company/product-	O-QUA-QCA6-051121/4999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5000
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5001
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/5002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5003
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5004
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5006
qca6421_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5007
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1936		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5009
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5010
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1967		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5012
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5013
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-051121/5014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
qca6426_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5015
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5016
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/5017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5018
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5019
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/5020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5021
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5022
Buffer Copy	20-Oct-21	7.2	Possible buffer overflow due	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5023
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5024
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5025
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5027
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5028
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5029
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of	https://www.qualcomm.	O-QUA-QCA6-051121/5030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	com/company/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5031
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5032
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/5033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	etins/octobe r-2021-bulletin	
Improper Authenticatio n	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-QCA6-051121/5034
qca6428_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-QCA6-051121/5035
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of	https://ww w.qualcomm.	O-QUA-QCA6-051121/5036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5037
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qca6430_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5039
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5040
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5042
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5043
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5045
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5046
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5048
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5049
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/5050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5051
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5052
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5053
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in	https://www.qualcomm.com/company/product-	O-QUA-QCA6-051121/5054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5055
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5056
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/5057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5058
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5059
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5061
qca6431_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5062
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1936		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5064
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5065
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1967		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5067
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5068
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-051121/5069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
qca6436_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5070
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5071
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/5072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5073
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5074
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/5075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5076
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5077
Buffer Copy	20-Oct-21	7.2	Possible buffer overflow due	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5078
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5079
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5080
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5082
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5083
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5084
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of	https://www.qualcomm.	O-QUA-QCA6-051121/5085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	com/company/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5086
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5087
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/5088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	etins/october-2021-bulletin	
qca6438_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5089
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5091
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5092
qca6564au_firmware					
Integer	20-Oct-21	7.2	Possible integer overflow	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5093
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5094
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5095
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/5096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5097
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5098
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5099
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5100
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5101
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length	https://www.qualcomm.	O-QUA-QCA6-051121/5102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5103
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5104
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QCA6-051121/5105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5106
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5107
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30310		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5109
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5110
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5111
qca6564a_firmware					
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null	https://www.qualcomm.	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	com/company/product-security/bulletins/october-2021-bulletin	051121/5112
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5113
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5114
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/5115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5116
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5118
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5119
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5120
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-051121/5121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5122
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5123
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5124
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QCA6-051121/5125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5126
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5127
Improper Restriction of Operations within the Bounds of a Memory	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-051121/5128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	r-2021-bulletin	
qca6564_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5129
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5130
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5132
qca6574au_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5133
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/5134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1917**	bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5135
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5136
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1949		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5138
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5139
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5141
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5142
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5144
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5145
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5147
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5148
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30288		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5150
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5151
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5152
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/5153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30305	bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5154
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5155
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5157
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5158
qca6574a_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5159
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-051121/5160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	r-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5161
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5162
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5164
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5165
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1967		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5167
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5168
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5170
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5171
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-051121/5172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5173
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5174
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5176
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5177
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5178
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/5179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	etins/octobe r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5180
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5181
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30312**		
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5183
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5184
qca6574_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5185
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/5186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5187
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5188
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5190
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5191
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5193
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5194
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in	https://www.qualcomm.com/company/product-	O-QUA-QCA6-051121/5195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5196
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5197
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5199
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5200
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6584au_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5202
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5203
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1968		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5205
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5206
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5208
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5209
Improper	20-Oct-21	5	Improper authentication of	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5210
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5211
qca6584_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6595au_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5213
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5214
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5216
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5217
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5218
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/5219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5220
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5221
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to	https://www.qualcomm.com/company/product-	O-QUA-QCA6-051121/5222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5223
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5225
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5226
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5227
Improper Input	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll	https://www.qualcomm.com/compan	O-QUA-QCA6-051121/5228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	y/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5229
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5230
Improper Restriction of Operations within the Bounds of a	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/5231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	etins/october-2021-bulletin	
qca6595_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5232
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5233
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5235
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5236
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5238
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5239
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5241
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5242
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/5243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5244
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5245
Use After	20-Oct-21	7.2	Improper handling of sensor	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5246
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5247
qca6694au_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5248
qca6694_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA6-051121/5249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5250
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5251
qca6696_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5252
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5253
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5254
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5255
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5256
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5257
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-051121/5258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5259
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5260
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-051121/5261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5262
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5264
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5265
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5266
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QCA6-051121/5267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5268
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA6-051121/5269
Improper Restriction of Operations within the Bounds of a Memory	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA6-051121/5270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	r-2021-bulletin	
qca7500_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA7-051121/5271
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA7-051121/5272
qca8072_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5273
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5274
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA8-051121/5275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5276
qca8075_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5278
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5279
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA8-051121/5280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	etins/october-2021-bulletin	
qca8081_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5281
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5283
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5284
qca8337_firmware					
Integer	20-Oct-21	7.2	Possible integer overflow	https://ww	O-QUA-QCA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5285
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5286
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5287
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery	https://www.qualcomm.com/company/product-	O-QUA-QCA8-051121/5288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5289
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5291
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5292
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA8-051121/5294
qca9367_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5295
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://www.qualcomm.com/compan	O-QUA-QCA9-051121/5296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5297
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5299
qca9369_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5300
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCA9-051121/5301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	bulletin	
qca9377_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5302
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5303
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5305
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5306
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5308
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5309
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30306		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5311
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5312
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30316**		
qca9379_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5314
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5315
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5317
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5318
qca9531_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QCA9-051121/5319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	security/bulletins/october-2021-bulletin	
qca9558_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5320
qca9561_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
qca9563_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5322
qca9880_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5324
qca9882_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5325
qca9886_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check	https://www.qualcomm.	O-QUA-QCA9-051121/5326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5327
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qca9887_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5329
qca9888_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5330
Out-of-	20-Oct-21	7.2	Possible stack overflow due	https://ww	O-QUA-QCA9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5331
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5332
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qca9889_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5334
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5336
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5337
qca9896_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA9-051121/5338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	etins/october-2021-bulletin	
qca9898_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5339
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5341
qca9980_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5342
Improper Authenticatio	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames	https://www.qualcomm.	O-QUA-QCA9-051121/5343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5344
qca9982_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
qca9984_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5346
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5347
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check	https://www.qualcomm.	O-QUA-QCA9-051121/5348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5349
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5351
qca9985_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5353
qca9990_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5354
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCA9-051121/5355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5356
qca9992_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5358
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5359
qca9994_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QCA9-051121/5360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5361
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCA9-051121/5362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qcm2290_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5363
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5364
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCM2-051121/5365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5366
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5367
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCM2-051121/5368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5369
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5370
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5371
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in	https://www.qualcomm.com/company/product-	O-QUA-QCM2-051121/5372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5373
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5374
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCM2-051121/5375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5376
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5377
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM2-051121/5378
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	O-QUA-QCM2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	051121/5379
qcm4290_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5380
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5382
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5383
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5385
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5386
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5388
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5389
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5391
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5392
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5393
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5395
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5396
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM4-051121/5398
qcm6125_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5399
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5401
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5402
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5403
Exposure of	20-Oct-21	2.1	Improper validation of	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	QCM6-051121/5404
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5405
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5407
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5408
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1984**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5410
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5411
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5412
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCM6-051121/5413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30258**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5414
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5415
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5417
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5418
qcm6490_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5420
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5421
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5422
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCM6-051121/5423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5424
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5425
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5426
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP	https://www.qualcomm.com/compan	O-QUA-QCM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	y/product-security/bulletins/october-2021-bulletin	051121/5427
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5428
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5429
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCM6-051121/5430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	r-2021-bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5431
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5432
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCM6-051121/5434
qcn5021_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5435
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5437
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
qcn5022_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5439
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5440
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information	https://www.qualcomm.com/company/product-	O-QUA-QCN5-051121/5441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5442
qcn5024_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5444
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5445
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	O-QUA-QCN5-051121/5446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	
qcn5052_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5447
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5449
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
qcn5054_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5451
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5452
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information	https://www.qualcomm.com/company/product-	O-QUA-QCN5-051121/5453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5454
qcn5064_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5456
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5457
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	O-QUA-QCN5-051121/5458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	
qcn5121_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5459
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5461
qcn5122_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5463
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5464
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-051121/5465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	etins/october-2021-bulletin	
qcn5124_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5466
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5468
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5469
qcn5152_firmware					
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	O-QUA-QCN5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5470
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5471
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5473
qcn5154_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5475
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5476
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCN5-051121/5477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
qcn5164_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5478
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5480
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5481
qcn5500_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check	https://www.qualcomm.	O-QUA-QCN5-051121/5482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	com/company/product-security/bulletins/october-2021-bulletin	
qcn5502_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5483
qcn5550_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCN5-051121/5484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5485
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30302		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN5-051121/5487
qcn6023_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN6-051121/5488
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN6-051121/5489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	etins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN6-051121/5490
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN6-051121/5491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qcn6024_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN6-051121/5492
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN6-051121/5493
Improper Authenticatio	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames	https://www.qualcomm.	O-QUA-QCN6-051121/5494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN6-051121/5495
qcn6122_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN6-051121/5496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN6-051121/5497
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN6-051121/5498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN6-051121/5499
qcn7605_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN7-051121/5500
qcn7606_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in	https://www.qualcomm.com/company/product-	O-QUA-QCN7-051121/5501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	security/bulletins/october-2021-bulletin	
qcn9000_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5502
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5504
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcn9012_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5506
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5507
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCN9-051121/5508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	bulletin	
qcn9022_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5509
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5511
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5512
qcn9024_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE	https://www.qualcomm.com/compan	O-QUA-QCN9-051121/5513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5514
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5516
qcn9070_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5517
Out-of-	20-Oct-21	7.2	Possible stack overflow due	https://ww	O-QUA-QCN9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5518
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5519
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qcn9072_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5521
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5523
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5524
qcn9074_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN9-051121/5525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5526
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5528
qcn9100_firmware					
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5529
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV	https://www.qualcomm.com/compan	O-QUA-QCN9-051121/5530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	y/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5531
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCN9-051121/5532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qcs2290_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5533
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5534
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCS2-051121/5535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5536
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5537
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS2-051121/5538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	etins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5539
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5540
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5541
Out-of-	20-Oct-21	7.2	Possible out of bound read or write in VR service due to	https://www.qualcomm.	O-QUA-QCS2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	com/company/product-security/bulletins/october-2021-bulletin	051121/5542
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5543
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5544
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS2-051121/5545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5546
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5547
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS2-051121/5549
qcs405_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5550
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5552
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5553
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5555
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5556
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS4-051121/5557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5558
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5560
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5561
qcs410_firmware					
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCS4-051121/5562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5563
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5564
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCS4-051121/5565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5566
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5567
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS4-051121/5568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5569
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5571
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5572
Improper Restriction of Operations within the Bounds of a	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS4-051121/5573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	etins/octobe r-2021-bulletin	
qcs4290_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-QCS4-051121/5574
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-QCS4-051121/5575
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided	https://ww w.qualcomm. com/compan	O-QUA-QCS4-051121/5576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	y/product-security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5577
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5578
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5580
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5582
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5583
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5584
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCS4-051121/5585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5586
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5587
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5589
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5590
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5591
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS4-051121/5592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
qcs603_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5593
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5594
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5596
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5597
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5599
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5600
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5601
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCS6-051121/5602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5603
qcs605_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5604
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5606
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5607
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5609
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5610
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5611
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR	https://www.qualcomm.com/company/product-	O-QUA-QCS6-051121/5612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5613
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5614
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5616
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5617
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5618
qcs610_firmware					
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause	https://www.qualcomm.com/compan	O-QUA-QCS6-051121/5619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	y/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5620
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5621
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-QCS6-051121/5622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5623
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5624
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS6-051121/5625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	etins/octobe r-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5626
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5628
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5629
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5630
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	O-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5631
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5632
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5633
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory	https://www.qualcomm.com/compan	O-QUA-QCS6-051121/5634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5635
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5636
Improper Restriction of Operations within the Bounds of a	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS6-051121/5637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	etins/octobe r-2021-bulletin	
qcs6125_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-QCS6-051121/5638
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-QCS6-051121/5639
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-QCS6-051121/5640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1959**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5641
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5642
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5644
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5645
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCS6-051121/5646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5647
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5648
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCS6-051121/5649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5650
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5651
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5652
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCS6-051121/5653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5654
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5655
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30297**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5657
qcs6490_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5658
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-QCS6-051121/5659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1917**	bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5660
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5661
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5662
Buffer Copy without Checking Size of Input	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in	https://www.qualcomm.com/company/product-	O-QUA-QCS6-051121/5663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5664
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5665
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5666
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR	https://www.qualcomm.com/compan	O-QUA-QCS6-051121/5667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5668
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5670
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5671
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCS6-051121/5672
Improper Restriction of Operations within the Bounds of a Memory	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QCS6-051121/5673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	r-2021-bulletin	
qcx315_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCX3-051121/5674
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCX3-051121/5675
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCX3-051121/5676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCX3-051121/5677
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCX3-051121/5678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QCX3-051121/5679
qet4101_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QET4-051121/5680
qrb5165_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QRB5-051121/5681
Out-of-	20-Oct-21	4.6	Possible stack buffer	https://ww	O-QUA-QRB5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5682
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QRB5-051121/5683
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QRB5-051121/5684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QRB5-051121/5685
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QRB5-051121/5686
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	O-QUA-QRB5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5687
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QRB5-051121/5688
qsm8250_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QSM8-051121/5689
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	O-QUA-QSM8-051121/5690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	
qsm8350_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QSM8-051121/5691
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QSM8-051121/5692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QSM8-051121/5693
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QSM8-051121/5694
qsw8573_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QSW8-051121/5695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QSW8-051121/5696
qualcomm215_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5697
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1936		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5699
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5700
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1967		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5702
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5703
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5704
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QUAL-051121/5705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5706
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5707
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5708
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-QUAL-051121/5709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-QUAL-051121/5710
sa415m_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA41-051121/5711
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA41-051121/5712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA41-051121/5713
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA41-051121/5714
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA41-051121/5715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	etins/october-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA41-051121/5716
sa515m_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA51-051121/5717
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://www.qualcomm.com/compan	O-QUA-SA51-051121/5718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA51-051121/5719
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA51-051121/5720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA51-051121/5721
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA51-051121/5722
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA51-051121/5723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30316**		
sa6145p_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5724
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5725
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5726
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-SA61-051121/5727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5728
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5729
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA61-051121/5730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	etins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5731
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5733
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5734
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5735
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SA61-051121/5736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5737
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5738
sa6150p_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SA61-051121/5739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5740
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5741
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5743
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5744
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1968		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5746
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5747
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5749
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5750
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5752
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5753
sa6155p_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5755
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5756
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5757
Integer Overflow or	20-Oct-21	7.2	Possible integer overflow due to improper check of	https://www.qualcomm.	O-QUA-SA61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	com/company/product-security/bulletins/october-2021-bulletin	051121/5758
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5759
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5760
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SA61-051121/5761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	r-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5762
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5763
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation	https://www.qualcomm.	O-QUA-SA61-051121/5764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5765
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5766
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	O-QUA-SA61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5767
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5768
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5769
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of	https://www.qualcomm.	O-QUA-SA61-051121/5770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5771
sa6155_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5772
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1949		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5774
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5775
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5777
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5778
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5780
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5781
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5782
Improper Input	20-Oct-21	5	Possible buffer overflow due to Improper validation of	https://www.qualcomm.	O-QUA-SA61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	com/company/product-security/bulletins/october-2021-bulletin	051121/5783
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5784
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA61-051121/5785
Improper Restriction of Operations within the	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence	https://www.qualcomm.com/company/product-	O-QUA-SA61-051121/5786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	security/bulletins/october-2021-bulletin	
sa8145p_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5787
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5788
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1949		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5790
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5791
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5793
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5794
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5796
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5797
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5798
Improper Input	20-Oct-21	5	Possible buffer overflow due to Improper validation of	https://www.qualcomm.	O-QUA-SA81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	com/company/product-security/bulletins/october-2021-bulletin	051121/5799
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5800
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5801
sa8150p_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5802
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5803
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5804
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in	https://www.qualcomm.com/company/product-	O-QUA-SA81-051121/5805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5806
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5807
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5809
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5810
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption	https://www.qualcomm.com/company/product-	O-QUA-SA81-051121/5811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5812
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5813
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length	https://www.qualcomm.com/compan	O-QUA-SA81-051121/5814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	y/product-security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5815
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5816
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto	https://www.qualcomm.com/company/product-	O-QUA-SA81-051121/5817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30315	security/bulletins/october-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5818
sa8155p_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5819
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5821
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5822
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5823
Buffer Copy without Checking Size	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination	https://www.qualcomm.com/compan	O-QUA-SA81-051121/5824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5825
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5826
Exposure of Resource to	20-Oct-21	2.1	Improper validation of kernel buffer address while	https://www.qualcomm.	O-QUA-SA81-051121/5827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5828
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5830
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5831
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5833
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5834
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5835
Improper Restriction of	20-Oct-21	7.2	Possible out of bound memory access due to	https://www.qualcomm.	O-QUA-SA81-051121/5836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	com/company/product-security/bulletins/october-2021-bulletin	
sa8155_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5837
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5838
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SA81-051121/5839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5840
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5841
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-1966**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5843
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5844
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5846
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5847
Out-of-	20-Oct-21	7.2	Possible stack overflow due	https://ww	O-QUA-SA81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5848
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5849
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5850
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SA81-051121/5851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5852
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5853
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**		
sa8195p_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5855
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5856
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5858
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5859
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5860
Buffer Copy without	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of	https://www.qualcomm.	O-QUA-SA81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	com/company/product-security/bulletins/october-2021-bulletin	051121/5861
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5862
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5863
Exposure of	20-Oct-21	2.1	Improper validation of	https://ww	O-QUA-SA81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5864
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5865
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5867
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5868
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5869
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in	https://www.qualcomm.com/company/product-	O-QUA-SA81-051121/5870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	security/bulletins/october-2021-bulletin	
Use After Free	20-Oct-21	7.2	Improper handling of sensor HAL structure in absence of sensor can lead to use after free in Snapdragon Auto **CVE ID : CVE-2021-30315**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5871
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SA81-051121/5872
sc8180x\\+sdx55_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SC81-051121/5873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SC81-051121/5874
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SC81-051121/5875
sc8280xp_firmware					
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	O-QUA-SC82-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5876
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SC82-051121/5877
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SC82-051121/5878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SC82-051121/5879
sd205_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD20-051121/5880
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD20-051121/5881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD20-051121/5882
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD20-051121/5883
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD20-051121/5884
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	O-QUA-SD20-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5885
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD20-051121/5886
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD20-051121/5887
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD20-051121/5888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD20-051121/5889
sd210_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD21-051121/5890
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD21-051121/5891
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD21-051121/5892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	etins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD21-051121/5893
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD21-051121/5894
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD21-051121/5895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD21-051121/5896
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD21-051121/5897
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD21-051121/5898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30291		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD21-051121/5899
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD21-051121/5900
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD21-051121/5901
sd429_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory	https://www.qualcomm.	O-QUA-SD42-051121/5902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	com/company/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD42-051121/5903
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD42-051121/5904
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD42-051121/5905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1959**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD42-051121/5906
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD42-051121/5907
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD42-051121/5908
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD42-051121/5909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	etins/octobe r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD42-051121/5910
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD42-051121/5911
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD42-051121/5912
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD42-051121/5913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	etins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD42-051121/5914
sd439_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD43-051121/5915
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD43-051121/5916
Integer Overflow or	20-Oct-21	7.2	Possible integer overflow due to improper check of	https://www.qualcomm.	O-QUA-SD43-051121/5917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD43-051121/5918
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD43-051121/5919
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD43-051121/5920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD43-051121/5921
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD43-051121/5922
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD43-051121/5923
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD43-051121/5924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD43-051121/5925
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD43-051121/5926
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD43-051121/5927
sd450_firmware					
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can	https://ww	O-QUA-SD45-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/5928
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD45-051121/5929
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD45-051121/5930
sd460_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD46-051121/5931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	etins/octobe r-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD46-051121/5932
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD46-051121/5933
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe	O-QUA-SD46-051121/5934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	r-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5935
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5936
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5938
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5939
Buffer Copy without Checking Size	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while	https://www.qualcomm.com/compan	O-QUA-SD46-051121/5940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5941
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5942
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5944
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5945
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5946
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory	https://www.qualcomm.com/compan	O-QUA-SD46-051121/5947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5948
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5949
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD46-051121/5950
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	O-QUA-SD46-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	051121/5951
sd480_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5952
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5953
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application	https://www.qualcomm.	O-QUA-SD48-051121/5954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	com/company/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5955
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5956
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE	https://www.qualcomm.com/compan	O-QUA-SD48-051121/5957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5958
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5959
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SD48-051121/5960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5961
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5962
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5963
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in	https://www.qualcomm.com/company/product-	O-QUA-SD48-051121/5964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5965
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5966
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD48-051121/5968
sd632_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD63-051121/5969
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD63-051121/5970
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while	https://www.qualcomm.com/compan	O-QUA-SD63-051121/5971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD63-051121/5972
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD63-051121/5973
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD63-051121/5974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD63-051121/5975
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD63-051121/5976
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD63-051121/5977
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD63-051121/5978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD63-051121/5979
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD63-051121/5980
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD63-051121/5981
sd660_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of	https://www.qualcomm.	O-QUA-SD66-051121/5982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5983
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5985
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5986
Improper Restriction of Operations within the	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence	https://www.qualcomm.com/company/product-	O-QUA-SD66-051121/5987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	security/bulletins/october-2021-bulletin	
sd662_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5988
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5989
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5991
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5992
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5994
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5995
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD66-051121/5996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5997
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/5998
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD66-051121/5999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6000
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6001
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6002
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD66-051121/6003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6004
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6005
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30297**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6007
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6008
sd665_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6009
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can	https://ww	O-QUA-SD66-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/6010
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6011
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6012
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD66-051121/6013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6014
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6015
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD66-051121/6016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6017
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6019
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6020
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6021
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD66-051121/6022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6023
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6024
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30288		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6026
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6027
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD66-051121/6028
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD66-051121/6029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	bulletin	
sd670_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6030
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6031
Out-of-	20-Oct-21	7.2	Possible stack overflow due	https://ww	O-QUA-SD67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/6032
sd675_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6033
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6035
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6036
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6037
Out-of-	20-Oct-21	7.2	Possible memory corruption	https://ww	O-QUA-SD67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/6038
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6039
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1968		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6041
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6042
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6044
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6045
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1985		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6047
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6048
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6049
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6051
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6052
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6054
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6055
sd678_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6056
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application	https://www.qualcomm.	O-QUA-SD67-051121/6057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	com/company/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6058
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6059
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://www.qualcomm.com/compan	O-QUA-SD67-051121/6060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6061
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6062
Exposure of	20-Oct-21	2.1	Improper validation of	https://ww	O-QUA-SD67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/6063
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6064
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6066
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6067
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6068
Out-of-	20-Oct-21	7.2	Possible stack overflow due to improper validation of	https://www.qualcomm.	O-QUA-SD67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	com/company/product-security/bulletins/october-2021-bulletin	051121/6069
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6070
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6071
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6073
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6074
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6075
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to	https://www.qualcomm.com/compan	O-QUA-SD67-051121/6076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	y/product-security/bulletins/october-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD67-051121/6077
sd690_5g_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6078
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD69-051121/6079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	etins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6080
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6081
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1966		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6083
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6084
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD69-051121/6085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6086
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6087
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1985**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6089
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6090
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6091
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD69-051121/6092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6093
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6094
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30297		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6096
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6097
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD69-051121/6098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd710_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD71-051121/6099
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD71-051121/6100
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD71-051121/6101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
sd712_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD71-051121/6102
sd720g_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6103
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6105
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6106
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6108
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6109
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD72-051121/6110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6111
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6113
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6114
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6115
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD72-051121/6116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6117
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6118
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6120
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6121
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6122
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD72-051121/6124
sd730_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6125
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6127
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6128
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6130
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6131
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6133
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6134
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6135
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6137
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6138
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6139
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	O-QUA-SD73-051121/6140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD73-051121/6141
sd750g_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6142
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD75-051121/6143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6144
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6145
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-1966**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6147
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6148
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD75-051121/6149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6150
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6151
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD75-051121/6152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6153
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6154
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6155
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD75-051121/6156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6157
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6158
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30297**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6160
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6161
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD75-051121/6162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
sd765g_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6163
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6164
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6165
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD76-051121/6166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	etins/octobe r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6167
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6168
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD76-051121/6169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6170
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6171
Buffer Copy without	20-Oct-21	7.2	Possible buffer overflow due to improper validation of	https://www.qualcomm.	O-QUA-SD76-051121/6172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6173
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6174
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6176
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6177
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6178
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of	https://www.qualcomm.	O-QUA-SD76-051121/6179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	com/company/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6180
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6181
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6183
sd765_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6184
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6186
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6187
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6188
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery	https://www.qualcomm.com/company/product-	O-QUA-SD76-051121/6189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6190
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6192
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6193
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6194
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR	https://www.qualcomm.com/company/product-	O-QUA-SD76-051121/6195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6196
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6197
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6199
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6200
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6201
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD76-051121/6202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	etins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6203
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6204
sd768g_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD76-051121/6205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	etins/octobe r-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD76-051121/6206
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD76-051121/6207
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD76-051121/6208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6209
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6210
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6212
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6213
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1984		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6215
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6216
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6217
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30258		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6219
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6220
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6221
Buffer Copy	20-Oct-21	3.6	Possible out of bound read	https://ww	O-QUA-SD76-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/6222
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6223
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD76-051121/6224
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD76-051121/6225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	bulletin	
sd778g_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6226
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6227
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD77-051121/6228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6229
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6230
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6232
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6233
Buffer Copy without Checking Size of Input	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in	https://www.qualcomm.com/company/product-	O-QUA-SD77-051121/6234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6235
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6236
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6238
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6239
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6240
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory	https://www.qualcomm.com/compan	O-QUA-SD77-051121/6241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6242
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6243
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6245
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6246
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD77-051121/6247
Improper Restriction of	20-Oct-21	7.2	Possible out of bound memory access due to	https://www.qualcomm.	O-QUA-SD77-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	com/company/product-security/bulletins/october-2021-bulletin	051121/6248
sd780g_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6249
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6250
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD78-051121/6251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6252
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6253
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6256
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD78-051121/6257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6258
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6259
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6260
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD78-051121/6261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6262
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6263
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD78-051121/6264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6265
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6266
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6268
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6269
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD78-051121/6270
sd7c_firmware					
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application	https://www.qualcomm.	O-QUA-SD7C-051121/6271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD7C-051121/6272
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD7C-051121/6273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD7C-051121/6274
sd820_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD82-051121/6275
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD82-051121/6276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD82-051121/6277
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD82-051121/6278
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV	https://www.qualcomm.com/compan	O-QUA-SD82-051121/6279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	y/product-security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD82-051121/6280
sd821_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD82-051121/6281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD82-051121/6282
sd835_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD83-051121/6283
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD83-051121/6284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD83-051121/6285
sd845_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD84-051121/6286
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD84-051121/6287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD84-051121/6288
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD84-051121/6289
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD84-051121/6290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD84-051121/6291
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD84-051121/6292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd850_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6293
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6294
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
sd855_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6296
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6297
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6299
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6300
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1959**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6302
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6303
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6305
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6306
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD85-051121/6307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6308
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6309
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD85-051121/6310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6311
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6312
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6313
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD85-051121/6314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6315
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6316
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30297**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD85-051121/6318
sd865_5g_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6319
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD86-051121/6320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1917**	bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6321
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6322
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6323
Buffer Copy without Checking Size	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination	https://www.qualcomm.com/compan	O-QUA-SD86-051121/6324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6325
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6327
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6328
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6329
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	O-QUA-SD86-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/6330
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6331
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6332
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6334
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6335
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6336
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	O-QUA-SD86-051121/6337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6338
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD86-051121/6339
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD86-051121/6340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	r-2021-bulletin	
sd870_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6341
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6342
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD87-051121/6343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	r-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6344
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6345
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6347
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6348
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6350
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6351
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6353
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6354
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6355
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6357
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6358
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6360
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6361
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD87-051121/6362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
sd888_5g_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6363
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6364
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1932		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6366
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6367
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6368
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery	https://www.qualcomm.com/company/product-	O-QUA-SD88-051121/6369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6370
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6372
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6373
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6374
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR	https://www.qualcomm.com/company/product-	O-QUA-SD88-051121/6375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6376
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6377
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6379
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6380
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6381
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD88-051121/6382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	etins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6383
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6384
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6386
sd888_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6387
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6388
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while	https://www.qualcomm.com/compan	O-QUA-SD88-051121/6389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6390
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6392
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6393
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6394
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD88-051121/6395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6396
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6397
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30288		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6399
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6400
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6401
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD88-051121/6402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6403
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD88-051121/6404
Improper Restriction of Operations within the Bounds of a Memory	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SD88-051121/6405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	r-2021-bulletin	
sda429w_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDA4-051121/6406
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDA4-051121/6407
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDA4-051121/6408
Out-of-	20-Oct-21	4.6	Possible stack buffer	https://ww	O-QUA-SDA4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	051121/6409
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDA4-051121/6410
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDA4-051121/6411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDA4-051121/6412
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDA4-051121/6413
sdm429w_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM4-051121/6414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1936		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM4-051121/6415
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM4-051121/6416
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM4-051121/6417
sdm630_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory	https://www.qualcomm.	O-QUA-SDM6-051121/6418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	com/company/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6419
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6420
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6422
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6423
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1984		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6425
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6426
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6427
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30258		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6429
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6430
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDM6-051121/6431
sdm830_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDM8-051121/6432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	etins/octobe r-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SDM8-051121/6433
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SDM8-051121/6434
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV	https://ww w.qualcomm. com/compan	O-QUA-SDM8-051121/6435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	y/product-security/bulletins/october-2021-bulletin	
sdw2500_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDW2-051121/6436
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDW2-051121/6437
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of	https://www.qualcomm.	O-QUA-SDW2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	com/company/product-security/bulletins/october-2021-bulletin	051121/6438
sdx12_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX1-051121/6439
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX1-051121/6440
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SDX1-051121/6441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX1-051121/6442
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX1-051121/6443
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX1-051121/6444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX1-051121/6445
sdx20m_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6446
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6448
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6449
sdx20_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in	https://www.qualcomm.com/company/product-	O-QUA-SDX2-051121/6450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6451
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6452
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV	https://www.qualcomm.com/compan	O-QUA-SDX2-051121/6453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	y/product-security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6454
sdx24_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1913**		
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6456
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6457
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX2-051121/6459
sdx50m_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6460
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6462
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6463
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6465
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6466
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1984**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6468
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6469
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6470
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SDX5-051121/6471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30258**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6472
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6473
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6475
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6476
sdx55m_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6478
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6479
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6480
Integer Overflow or	20-Oct-21	7.2	Possible integer overflow due to improper check of	https://www.qualcomm.	O-QUA-SDX5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	com/company/product-security/bulletins/october-2021-bulletin	051121/6481
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6482
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6483
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SDX5-051121/6484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	r-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6485
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6486
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation	https://www.qualcomm.	O-QUA-SDX5-051121/6487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	com/company/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6488
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1983		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6490
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6491
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6492
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SDX5-051121/6493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6494
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6495
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6497
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6498
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6499
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length	https://www.qualcomm.com/compan	O-QUA-SDX5-051121/6500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	y/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6501
sdx55_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6502
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in	https://www.qualcomm.com/compan	O-QUA-SDX5-051121/6503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	y/product-security/bulletins/october-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6504
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6505
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SDX5-051121/6506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6507
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6508
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6510
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6511
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SDX5-051121/6512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6513
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6514
Buffer Copy without Checking Size	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing	https://www.qualcomm.com/compan	O-QUA-SDX5-051121/6515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6516
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6517
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6518
Out-of-	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation	https://www.qualcomm.	O-QUA-SDX5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	com/company/product-security/bulletins/october-2021-bulletin	051121/6519
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6520
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6521
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SDX5-051121/6522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6523
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6524
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SDX5-051121/6525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6526
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDX5-051121/6527
sdx57m_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDX5-051121/6528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	etins/octobe r-2021-bulletin	
sdxr1_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SDXR-051121/6529
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SDXR-051121/6530
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SDXR-051121/6531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6532
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6533
Buffer Copy without Checking Size	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while	https://www.qualcomm.com/compan	O-QUA-SDXR-051121/6534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6535
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6536
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6538
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6539
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6540
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory	https://www.qualcomm.com/compan	O-QUA-SDXR-051121/6541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6542
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6543
sdxr2_5g_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6545
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6546
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6547
Out-of-	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check	https://www.qualcomm.	O-QUA-SDXR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	com/company/product-security/bulletins/october-2021-bulletin	051121/6548
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6549
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6551
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6552
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6553
Out-of-	20-Oct-21	7.2	Possible stack overflow due to improper validation of	https://www.qualcomm.	O-QUA-SDXR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	com/company/product-security/bulletins/october-2021-bulletin	051121/6554
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6555
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6556
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6558
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6559
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6560
Improper Authenticatio	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user	https://www.qualcomm.com/compan	O-QUA-SDXR-051121/6561

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	y/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SDXR-051121/6562
sd_455_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_4-051121/6563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_4-051121/6564
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_4-051121/6565
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_4-051121/6566
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD_4-051121/6567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD_4-051121/6568
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD_4-051121/6569
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD_4-051121/6570
sd_636_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory	https://ww w.qualcomm.	O-QUA-SD_6-051121/6571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	com/company/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6572
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6573
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6575
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6576
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1984		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6578
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6579
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6580
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30258		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6582
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6583
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6584
sd_675_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD_6-051121/6585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	etins/octobe r-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD_6-051121/6586
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD_6-051121/6587
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-SD_6-051121/6588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6589
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6590
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6592
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6593
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SD_6-051121/6594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6595
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6596
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD_6-051121/6597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6598
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6599
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-051121/6600
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD_6-051121/6601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-061121/6602
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-061121/6603
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD_6-061121/6604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-061121/6605
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_6-061121/6606
sd_8cx_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD_8-061121/6607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6608
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6609
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD_8-061121/6610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6611
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6612
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to	https://www.qualcomm.com/company/product-	O-QUA-SD_8-061121/6613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6614
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6616
sd_8c_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6617
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD_8-061121/6618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6619
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6620
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SD_8-061121/6621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6622
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6623
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV	https://www.qualcomm.com/compan	O-QUA-SD_8-061121/6624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	y/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SD_8-061121/6625
sm4125_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6627
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6628
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6630
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6631
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6633
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6634
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6636
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6637
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6638
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6640
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6641
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6642
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	O-QUA-SM41-061121/6643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM41-061121/6644
sm6250p_firmware					
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6646
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6647
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6648
Out-of-	20-Oct-21	6.4	Possible buffer over read due to lack of length check	https://www.qualcomm.	O-QUA-SM62-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	com/company/product-security/bulletins/october-2021-bulletin	061121/6649
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6650
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6651
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service	https://www.qualcomm.com/compan	O-QUA-SM62-061121/6652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6653
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6654
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM62-061121/6655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	etins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6656
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6657
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30312**		
sm6250_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6659
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6660
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1936		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6662
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6663
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1967		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6665
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6666
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6668
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6669
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-SM62-061121/6670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6671
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6672
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6673
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM62-061121/6674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	etins/octobe r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6675
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6676
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SM62-061121/6677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6678
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6679
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM62-061121/6680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30316**		
sm7250_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6681
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6682
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6683
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-SM72-061121/6684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6685
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6686
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM72-061121/6687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6688
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6689
Buffer Copy	20-Oct-21	7.2	Possible buffer overflow due	https://ww	O-QUA-SM72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	061121/6690
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6691
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6692
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6694
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6695
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6696
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of	https://www.qualcomm.	O-QUA-SM72-061121/6697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	com/company/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6698
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6699
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM72-061121/6701
sm7325_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6702
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-SM73-061121/6703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1917**	bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6704
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6705
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6706
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of	https://www.qualcomm.com/compan	O-QUA-SM73-061121/6707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6708
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6710
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6711
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6712
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before	https://www.qualcomm.com/compan	O-QUA-SM73-061121/6713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6714
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6715
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6717
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6718
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6719
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information	https://www.qualcomm.com/company/product-	O-QUA-SM73-061121/6720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	security/bulletins/october-2021-bulletin	
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6721
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6722
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-SM73-061121/6724
wcd9306_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6725
wcd9326_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6727
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6728
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-WCD9-061121/6729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6730
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6731
Improper	20-Oct-21	5	Possible buffer overflow due	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCD9-061121/6732
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6733
wcd9330_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6735
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6736
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6738
wcd9335_firmware					
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6739
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCD9-061121/6740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6741
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6742
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCD9-061121/6743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6744
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1980		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6746
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6747
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6748
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-WCD9-061121/6749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6750
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6751
wcd9340_firmware					
Integer Overflow or	20-Oct-21	7.2	Possible integer overflow due to improper length	https://www.qualcomm.	O-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	com/company/product-security/bulletins/october-2021-bulletin	061121/6752
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6753
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6755
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6756
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1968		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6758
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6759
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6761
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30302		
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6763
wcd9341_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6764
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6766
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6767
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6769
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6770
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCD9-061121/6771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6772
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6774
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6775
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6776
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-061121/6777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	etins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6778
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6779
wcd9360_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace	https://www.qualcomm.com/compan	O-QUA-WCD9-061121/6780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	y/product-security/bulletins/october-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6781
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6782
Out-of-	20-Oct-21	7.2	Possible stack overflow due	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCD9-061121/6783
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6784
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6786
wcd9370_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6787
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1917		
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6789
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6790
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6792
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6793
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6794
Exposure of	20-Oct-21	2.1	Improper validation of	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCD9-061121/6795
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6796
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6798
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6799
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1984**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6801
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6802
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6803
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCD9-061121/6804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30258**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6805
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6806
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6808
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6809
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6810
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-061121/6811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	etins/octobe r-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCD9-061121/6812
Improper Authenticatio n	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCD9-061121/6813
Improper Restriction of Operations within the Bounds of a Memory	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe	O-QUA-WCD9-061121/6814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	r-2021-bulletin	
wcd9371_firmware					
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6815
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6816
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCD9-061121/6817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6818
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6819
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCD9-061121/6820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6821
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6822
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6823
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV	https://www.qualcomm.com/compan	O-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	y/product-security/bulletins/october-2021-bulletin	061121/6824
wcd9375_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6825
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6826
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application	https://www.qualcomm.	O-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	com/company/product-security/bulletins/october-2021-bulletin	061121/6827
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6828
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6829
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://www.qualcomm.com/compan	O-QUA-WCD9-061121/6830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6831
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6832
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to	https://www.qualcomm.com/company/product-	O-QUA-WCD9-061121/6833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	security/bulletins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6834
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1977		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6836
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6837
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6839
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6840
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6841
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6843
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6844
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6845
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	O-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	061121/6846
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6847
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6848
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCD9-061121/6849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile **CVE ID : CVE-2021-30306**	bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6850
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6851
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**		
wcd9380_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6853
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6854
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1932**		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6856
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6857
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6858
Buffer Copy without	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of	https://www.qualcomm.	O-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	com/company/product-security/bulletins/october-2021-bulletin	061121/6859
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6860
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6861
Exposure of	20-Oct-21	2.1	Improper validation of	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCD9-061121/6862
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6863
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6865
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6866
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6867
Out-of-	20-Oct-21	7.2	Possible stack overflow due to improper validation of	https://www.qualcomm.	O-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	com/company/product-security/bulletins/october-2021-bulletin	061121/6868
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6869
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6870
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6872
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6873
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6874
Improper Authenticatio	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user	https://www.qualcomm.com/compan	O-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	y/product-security/bulletins/october-2021-bulletin	061121/6875
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6876
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6877
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6879
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6880
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30316		
wcd9385_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6882
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6883
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1932		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6885
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6886
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6887
Buffer Copy without Checking Size of Input	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in	https://www.qualcomm.com/company/product-	O-QUA-WCD9-061121/6888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6889
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6890
Out-of-	20-Oct-21	6.4	Possible buffer over read	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCD9-061121/6891
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6893
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length	https://www.qualcomm.	O-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	com/company/product-security/bulletins/october-2021-bulletin	061121/6894
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6895
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6896
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6897
Out-of-	20-Oct-21	7.2	Possible stack overflow due to improper length check of	https://www.qualcomm.	O-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	com/company/product-security/bulletins/october-2021-bulletin	061121/6898
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6899
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6900
Buffer Copy without Checking Size of Input	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR	https://www.qualcomm.com/company/product-	O-QUA-WCD9-061121/6901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	security/bulletins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6902
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6903
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCD9-061121/6904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30305	bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6905
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6906
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCD9-061121/6908
wcn3610_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6909
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6910
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6912
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6913
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6915
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6916
Buffer Copy without Checking Size	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while	https://www.qualcomm.com/compan	O-QUA-WCN3-061121/6917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6918
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6919
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6921
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6922
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6923
Buffer Copy without	20-Oct-21	3.6	Possible out of bound read due to improper validation	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	com/company/product-security/bulletins/october-2021-bulletin	061121/6924
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6925
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6926
Improper	20-Oct-21	7.2	Possible out of bound	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCN3-061121/6927
wcn3615_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6928
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6929
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6931
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6932
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6934
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6935
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-061121/6936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	etins/octobe r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/6937
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/6938
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/6939
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	O-QUA-WCN3-061121/6940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6941
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6942
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-061121/6943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6944
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6945
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6946
Improper Authenticatio	20-Oct-21	5	Improper authentication of sub-frames of a multicast	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	com/company/product-security/bulletins/october-2021-bulletin	061121/6947
wcn3620_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6948
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6949
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	com/company/product-security/bulletins/october-2021-bulletin	061121/6950
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6951
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6953
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6954
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6956
wcn3660b_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6957
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6958
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-061121/6959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6960
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6961
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-061121/6962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	r-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6963
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6964
Buffer Copy	20-Oct-21	7.2	Possible buffer overflow due	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCN3-061121/6965
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6966
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6967
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT **CVE ID : CVE-2021-30256**		
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6969
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6970
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6972
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6973
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6974
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6976
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6977
wcn3660_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-061121/6978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	r-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6979
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6980
wcn3680b_firmware					
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6982
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6983
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6984
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-061121/6985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6986
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6988
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6989
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6990
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-061121/6991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	etins/octobe r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6992
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6993
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6995
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6996
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6997
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-061121/6998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	r-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/6999
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7000
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCN3-061121/7001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	bulletin	
wcn3680_firmware					
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7002
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7003
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1959		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7005
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7006
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7007
Out-of-	20-Oct-21	3.6	Possible buffer over read	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCN3-061121/7008
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7009
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7010
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7012
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7013
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7014
wcn3910_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCN3-061121/7015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	bulletin	
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7016
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7017
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1936**		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7019
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7020
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7022
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7023
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1984**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7025
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7026
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7027
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCN3-061121/7028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30258**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7029
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7030
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7032
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7033
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30312		
wcn3950_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7035
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7036
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1932		
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7038
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7039
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7040
Buffer Copy without Checking Size of Input	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in	https://www.qualcomm.com/company/product-	O-QUA-WCN3-061121/7041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7042
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7043
Exposure of Resource to Wrong	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to	https://www.qualcomm.com/compan	O-QUA-WCN3-061121/7044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7045
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7047
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7048
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7049
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR	https://www.qualcomm.com/company/product-	O-QUA-WCN3-061121/7050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7051
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7052
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7054
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7055
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7056
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-061121/7057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	etins/octobe r-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/7058
Improper Authenticatio n	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/7059
Improper Restriction of Operations within the Bounds of a Memory	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe	O-QUA-WCN3-061121/7060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	r-2021-bulletin	
wcn3980_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7061
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7062
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-WCN3-061121/7063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7064
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7065
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-061121/7066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	etins/october-2021-bulletin	
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7067
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7069
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7070
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCN3-061121/7071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7072
wcn3988_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7073
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-061121/7074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	etins/octobe r-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/7075
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/7076
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/7077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7078
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7079
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7081
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7082
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7084
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7085
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-061121/7086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	etins/octobe r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/7087
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/7088
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/7089
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	O-QUA-WCN3-061121/7090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7091
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7092
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN3-061121/7093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7094
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7095
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7096
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCN3-061121/7097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7098
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7099
wcn3990_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-061121/7100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	etins/octobe r-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/7101
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN3-061121/7102
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of	https://ww w.qualcomm. com/compan	O-QUA-WCN3-061121/7103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7104
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7106
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7107
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-061121/7108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	etins/october-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7109
wcn3991_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7110
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in	https://www.qualcomm.com/compan	O-QUA-WCN3-061121/7111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	y/product-security/bulletins/october-2021-bulletin	
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7112
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7113
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCN3-061121/7114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7115
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7116
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7118
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7119
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCN3-061121/7120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7121
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7122
Buffer Copy without Checking Size	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing	https://www.qualcomm.com/compan	O-QUA-WCN3-061121/7123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7124
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7125
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7126
Out-of-	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	com/company/product-security/bulletins/october-2021-bulletin	061121/7127
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7128
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7129
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-WCN3-061121/7130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7131
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7132
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7133
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-061121/7134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	etins/october-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7135
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7136
wcn3998_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace	https://www.qualcomm.com/compan	O-QUA-WCN3-061121/7137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	y/product-security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7138
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7139
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-WCN3-061121/7140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	security/bulletins/october-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7141
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7142
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-1966**		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7144
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7145
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7147
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7148
Buffer Copy	20-Oct-21	7.2	Possible buffer overflow due	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WCN3-061121/7149
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7150
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7151
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT **CVE ID : CVE-2021-30256**		
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7153
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7154
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7156
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7157
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7158
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7160
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7161
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7163
wcn3999_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7164
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7166
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7167
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7169
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7170
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption	https://www.qualcomm.com/company/product-	O-QUA-WCN3-061121/7171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7172
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN3-061121/7174
wcn6740_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7175
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-WCN6-061121/7176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	security/bulletins/october-2021-bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7177
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7178
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7180
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7181
Buffer Copy without Checking Size of Input	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in	https://www.qualcomm.com/company/product-	O-QUA-WCN6-061121/7182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7183
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7184
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7186
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7187
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7188
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory	https://www.qualcomm.com/compan	O-QUA-WCN6-061121/7189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7190
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7191
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7193
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7194
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7195
Improper Restriction of	20-Oct-21	7.2	Possible out of bound memory access due to	https://www.qualcomm.	O-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	com/company/product-security/bulletins/october-2021-bulletin	061121/7196
wcn6750_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7197
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7198
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCN6-061121/7199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7200
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7201
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7203
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7204
Buffer Copy without Checking Size of Input	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in	https://www.qualcomm.com/company/product-	O-QUA-WCN6-061121/7205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7206
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7207
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7209
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7210
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7211
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory	https://www.qualcomm.com/compan	O-QUA-WCN6-061121/7212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7213
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7214
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7216
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7217
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7218
Improper Restriction of	20-Oct-21	7.2	Possible out of bound memory access due to	https://www.qualcomm.	O-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	com/company/product-security/bulletins/october-2021-bulletin	061121/7219
wcn6850_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7220
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7221
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WCN6-061121/7222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	bulletin	
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7223
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7224
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7226
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7227
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7229
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7230
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN6-061121/7231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	etins/octobe r-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN6-061121/7232
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN6-061121/7233
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN6-061121/7234
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	O-QUA-WCN6-061121/7235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7236
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7237
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN6-061121/7238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7239
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7240
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30304		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7242
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7243
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7244
Improper Restriction of Operations within the Bounds of a	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN6-061121/7245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	etins/october-2021-bulletin	
wcn6851_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7246
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7247
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1936		
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7249
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7250
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7251
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of	https://www.qualcomm.com/compan	O-QUA-WCN6-061121/7252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7253
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7256
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7257
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before	https://www.qualcomm.com/compan	O-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	y/product-security/bulletins/october-2021-bulletin	061121/7258
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7259
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7260
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7262
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7263
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7264
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information	https://www.qualcomm.com/company/product-	O-QUA-WCN6-061121/7265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	security/bulletins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7266
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7267
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7269
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7270
wcn6855_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1913**		
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7272
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7273
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7274
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN6-061121/7275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7276
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7277
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check	https://www.qualcomm.	O-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	com/company/product-security/bulletins/october-2021-bulletin	061121/7278
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7279
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7280
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service	https://www.qualcomm.com/compan	O-QUA-WCN6-061121/7281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7282
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7283
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7284
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV	https://www.qualcomm.com/compan	O-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	y/product-security/bulletins/october-2021-bulletin	061121/7285
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7286
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7287
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN6-061121/7288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	etins/octobe r-2021-bulletin	
Improper Authenticatio n	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN6-061121/7289
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN6-061121/7290
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WCN6-061121/7291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7292
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7293
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7294
wcn6856_firmware					
Integer Overflow or	20-Oct-21	7.2	Possible integer overflow due to improper length	https://www.qualcomm.	O-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	com/company/product-security/bulletins/october-2021-bulletin	061121/7295
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7296
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7297
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7299
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7300
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7302
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7303
Buffer Copy without Checking Size of Input ('Classic	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN6-061121/7304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	etins/october-2021-bulletin	
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7305
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7306
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7307
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-WCN6-061121/7308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7309
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7310
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WCN6-061121/7311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	r-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7312
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7313
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30304		
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7315
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7316
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WCN6-061121/7317
Improper Restriction of Operations within the Bounds of a	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN6-061121/7318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	etins/octobe r-2021-bulletin	
whs9410_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WHS9-061121/7319
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://ww w.qualcomm. com/compan y/product-security/bull etins/octobe r-2021-bulletin	O-QUA-WHS9-061121/7320
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon	https://ww w.qualcomm. com/compan	O-QUA-WHS9-061121/7321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	y/product-security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WHS9-061121/7322
wsa8810_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1913		
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7324
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7325
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1966		
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7327
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7328
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**		
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7330
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7331
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of	https://www.qualcomm.	O-QUA-WSA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	com/company/product-security/bulletins/october-2021-bulletin	061121/7332
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7333
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7335
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7336
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30316		
wsa8815_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7338
Incorrect Authorization	20-Oct-21	7.2	Improper access control in trusted application environment can cause unauthorized access to CDSP or ADSP VM memory with either privilege in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1932**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7339
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7341
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7342
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1968**		
Exposure of Resource to Wrong Sphere	20-Oct-21	2.1	Improper validation of kernel buffer address while copying information back to user buffer can lead to kernel memory information exposure to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1969**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7344
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7345
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-WSA8-061121/7346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7347
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**		
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7349
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7350
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-30312**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7352
wsa8830_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7353
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7354
NULL Pointer	20-Oct-21	7.8	Null pointer dereference can	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WSA8-061121/7355
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7356
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7357
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WSA8-061121/7358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	r-2021-bulletin	
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7359
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7360
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE	https://www.qualcomm.com/compan	O-QUA-WSA8-061121/7361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**	y/product-security/bulletins/october-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7362
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7363
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-WSA8-061121/7364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7365
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7366
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7367
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in	https://www.qualcomm.com/company/product-	O-QUA-WSA8-061121/7368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**	security/bulletins/october-2021-bulletin	
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7369
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7370
Buffer Copy without Checking Size of Input ('Classic Buffer	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WSA8-061121/7371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	r-2021-bulletin	
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7372
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7373
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7375
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7376
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7377
Improper	20-Oct-21	7.2	Possible out of bound	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	w.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	WSA8-061121/7378
wsa8835_firmware					
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper length check while updating grace period and count record in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1913**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7379
NULL Pointer Dereference	20-Oct-21	7.2	Null pointer dereference can occur due to memory allocation failure in DIAG in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1917**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7380
NULL Pointer Dereference	20-Oct-21	7.8	Null pointer dereference can occur due to lack of null check for user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WSA8-061121/7381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1936**	r-2021-bulletin	
Integer Overflow or Wraparound	20-Oct-21	7.2	Possible integer overflow due to improper check of batch count value while sanitizer is enabled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1949**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7382
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of bound check of input index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1959**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7383
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	4.6	Possible buffer overflow due to lack of length check of source and destination buffer before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1966**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	4.6	Possible stack buffer overflow due to lack of check on the maximum number of post NAN discovery attributes while processing a NAN Match event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1967**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7385
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to improper validation of frame length while processing AEAD decryption during ASSOC response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1977**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7386
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer over read due to lack of length check while parsing beacon IE response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1980**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper handling of negative data length while processing write request in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1983**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7388
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	7.2	Possible buffer overflow due to improper validation of index value while processing the plugin block in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1984**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7389
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to lack of data length check in QVR Service configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1985**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper validation of camera name length before copying the name in VR Service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30256**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7391
Out-of-bounds Read	20-Oct-21	7.2	Possible out of bound read or write in VR service due to lack of validation of DSP selection values in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT **CVE ID : CVE-2021-30257**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7392
Out-of-bounds Write	20-Oct-21	7.2	Possible buffer overflow due to improper size calculation of payload received in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30258**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7393
Out-of-bounds Write	20-Oct-21	7.2	Possible stack overflow due to improper length check of TLV while copying the TLV to a local stack variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30288**		
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30291**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7395
Out-of-bounds Write	20-Oct-21	7.2	Possible memory corruption due to lack of validation of client data used for memory allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30292**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7396
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Oct-21	3.6	Possible out of bound read due to improper validation of packet length while handling data transfer in VR service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-30297**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Oct-21	5	Improper authentication of EAP WAPI EAPOL frames from unauthenticated user can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30302**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7398
Out-of-bounds Read	20-Oct-21	6.4	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity **CVE ID : CVE-2021-30304**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7399
Improper Input Validation	20-Oct-21	4.6	Possible out of bound access due to lack of validation of page offset before page is inserted in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30305**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7400
Out-of-bounds Read	20-Oct-21	3.6	Possible buffer over read due to improper buffer allocation for file length passed from user space in Snapdragon Auto, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octobe	O-QUA-WSA8-061121/7401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-30306**	r-2021-bulletin	
Improper Input Validation	20-Oct-21	5	Possible buffer overflow due to Improper validation of received CF-ACK and CF-Poll data frames in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-30310**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7402
Improper Authentication	20-Oct-21	5	Improper authentication of sub-frames of a multicast AMSDU frame can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-30312**	https://www.qualcomm.com/company/product-security/bulletins/october-2021-bulletin	O-QUA-WSA8-061121/7403
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-21	7.2	Possible out of bound memory access due to improper boundary check while creating HSYNC fence in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2021-	O-QUA-WSA8-061121/7404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-30316**	bulletin	
Redhat					
enterprise_linux					
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-Oct-21	7.1	A flaw was found in the libtpms code that may cause access beyond the boundary of internal buffers. The vulnerability is triggered by specially-crafted TPM2 command packets that then trigger the issue when the state of the TPM2's volatile state is written. The highest threat from this vulnerability is to system availability. This issue affects libtpms versions before 0.8.5, before 0.7.9 and before 0.6.6. **CVE ID : CVE-2021-3746**	https://bugzilla.redhat.com/show_bug.cgi?id=1998588	O-RED-ENTE-061121/7405
skyworth					
penguin_aurora_box_firmware					
Incorrect Authorization	26-Oct-21	6.4	Penguin Aurora TV Box 41502 is a high-end network HD set-top box produced by Tencent Video and Skyworth Digital. An unauthorized access vulnerability exists in the Penguin Aurora Box. An attacker can use the vulnerability to gain unauthorized access to a specific link to remotely control the TV. **CVE ID : CVE-2021-41873**	N/A	O-SKY-PENG-061121/7406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Trane					
tracer_sc\\+_firmware					
Improper Input Validation	27-Oct-21	6.5	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software. **CVE ID : CVE-2021-38450**	https://us-cert.cisa.gov/ics/advisories/icsa-21-266-02	O-TRA-TRAC-061121/7407
tracer_sc_firmware					
Improper Input Validation	27-Oct-21	6.5	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software. **CVE ID : CVE-2021-38450**	https://us-cert.cisa.gov/ics/advisories/icsa-21-266-02	O-TRA-TRAC-061121/7408
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-21	4.3	The affected product's web application does not properly neutralize the input during webpage generation, which could allow an attacker to inject code in the input forms. **CVE ID : CVE-2021-42534**	https://us-cert.cisa.gov/ics/advisories/icsa-21-292-02	O-TRA-TRAC-061121/7409
zephyrproject					
zephyr					
N/A	19-Oct-21	5	Truncated L2CAP K-frame causes assertion failure. Zephyr versions >= 2.4.0, >= v.2.50 contain Improper Handling of Length Parameter Inconsistency (CWE-130), Reachable Assertion (CWE-617). For	http://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-fx88-6c29-vrp3	O-ZEP-ZEPH-061121/7410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-fx88-6c29-vrp3 **CVE ID : CVE-2021-3454**		
Use After Free	19-Oct-21	5	Disconnecting L2CAP channel right after invalid ATT request leads freeze. Zephyr versions >= 2.4.0, >= 2.5.0 contain Use After Free (CWE-416). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-7g38-3x9v-v7vp **CVE ID : CVE-2021-3455**	N/A	O-ZEP-ZEPH-061121/7411
ZTE					
mf971r_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Oct-21	4.3	ZTE MF971R product has a CRLF injection vulnerability. An attacker could exploit the vulnerability to modify the HTTP response header information through a specially crafted HTTP request. **CVE ID : CVE-2021-21743**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	O-ZTE-MF97-061121/7412
N/A	20-Oct-21	5	ZTE MF971R product has a configuration file control vulnerability. An attacker could use this vulnerability to modify the configuration parameters of the device, causing some security functions of the device to be disabled.	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	O-ZTE-MF97-061121/7413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21744		
Improper Authentication	20-Oct-21	4.3	ZTE MF971R product has a Referer authentication bypass vulnerability. Without CSRF verification, an attackercould use this vulnerability to perform illegal authorization operations by sending a request to the user to click. **CVE ID : CVE-2021-21745**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	O-ZTE-MF97-061121/7414
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-21	4.3	ZTE MF971R product has reflective XSS vulnerability. An attacker could use the vulnerability to obtain cookie information. **CVE ID : CVE-2021-21746**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	O-ZTE-MF97-061121/7415
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-21	4.3	ZTE MF971R product has reflective XSS vulnerability. An attacker could use the vulnerability to obtain cookie information. **CVE ID : CVE-2021-21747**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	O-ZTE-MF97-061121/7416
Out-of-bounds Write	20-Oct-21	7.5	ZTE MF971R product has two stack-based buffer overflow vulnerabilities. An attacker could exploit the vulnerabilities to execute arbitrary code. **CVE ID : CVE-2021-21748**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764	O-ZTE-MF97-061121/7417
Out-of-bounds Write	20-Oct-21	7.5	ZTE MF971R product has two stack-based buffer overflow vulnerabilities. An attacker could exploit the vulnerabilities to execute	https://support.zte.com.cn/support/news/LoopholeInfoDetail.a	O-ZTE-MF97-061121/7418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code. **CVE ID : CVE-2021-21749**	spx?newsId=1019764	