Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
activefusions					
order_status_batch_change					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-21	4.3	Cross-site scripting vulnerability in Order Status Batch Change Plug-in (for EC-CUBE 3.0 series) all versions allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20828**	N/A	A-ACT-ORDE-061021/1
activemedia					
microcopy					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The edit functionality in the MicroCopy WordPress plugin through 1.1.0 makes a get request to fetch the related option. The id parameter used is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. **CVE ID : CVE-2021-24397**	N/A	A-ACT-MICR-061021/2
Adobe					
creative_cloud_desktop_application					
Improper Input Validation	29-Sep-21	4.6	Adobe Creative Cloud Desktop Application for macOS version 5.3 (and earlier) is affected by a privilege escalation vulnerability that could allow a normal user to delete the OOBE directory and get	https://helpx.adobe.com/security/products/creative-cloud/apsb21-18.html	A-ADO-CREA-061021/3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permissions of any directory under the administrator authority. **CVE ID : CVE-2021-28547**		
digital_editions					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Sep-21	9.3	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary command execution vulnerability. An authenticated attacker could leverage this vulnerability to execute arbitrary commands. User interaction is required to abuse this vulnerability in that a user must open a maliciously crafted .epub file. **CVE ID : CVE-2021-39826**	https://helpx.adobe.com/security/products/Digital-Editions/apsb21-80.html	A-ADO-DIGI-061021/4
Creation of Temporary File in Directory with Insecure Permissions	27-Sep-21	6.8	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary file write vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to write an arbitrary file to the system. User interaction is required before product installation to abuse this vulnerability. **CVE ID : CVE-2021-39827**	https://helpx.adobe.com/security/products/Digital-Editions/apsb21-80.html	A-ADO-DIGI-061021/5
Creation of Temporary File in Directory with Insecure Permissions	27-Sep-21	6.8	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by a privilege escalation vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to escalate privileges. User	https://helpx.adobe.com/security/products/Digital-Editions/apsb21-80.html	A-ADO-DIGI-061021/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is required before product installation to abuse this vulnerability. **CVE ID : CVE-2021-39828**		
experience_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	4.3	Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a stored XSS vulnerability when creating Content Fragments. An authenticated attacker can send a malformed POST request to achieve server-side denial of service. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2021-40711**	https://helpx.adobe.com/security/products/experience-manager/apsb21-82.html	A-ADO-EXPE-061021/7
Improper Input Validation	27-Sep-21	4	Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a improper input validation vulnerability via the path parameter. An authenticated attacker can send a malformed POST request to achieve server-side denial of service. **CVE ID : CVE-2021-40712**	https://helpx.adobe.com/security/products/experience-manager/apsb21-82.html	A-ADO-EXPE-061021/8
Improper Certificate Validation	27-Sep-21	4.3	Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a improper certificate validation vulnerability in the cold storage component. If an attacker can achieve a man in the middle when the cold server establishes a new	https://helpx.adobe.com/security/products/experience-manager/apsb21-82.html	A-ADO-EXPE-061021/9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certificate, they would be able to harvest sensitive information. **CVE ID : CVE-2021-40713**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	4.3	Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability via the accesskey parameter. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser **CVE ID : CVE-2021-40714**	https://helpx.adobe.com/security/products/experience-manager/apsb21-82.html	A-ADO-EXPE-061021/10
incopy					
Access of Memory Location After End of Buffer	27-Sep-21	6.8	Adobe InCopy version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious TIFF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. **CVE ID : CVE-2021-39818**	https://helpx.adobe.com/security/products/incopy/apsb21-71.html	A-ADO-INCO-061021/11
Access of Memory Location After End of Buffer	27-Sep-21	6.8	Adobe InCopy version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious XML file, potentially resulting in arbitrary code execution in the context of the current	https://helpx.adobe.com/security/products/incopy/apsb21-71.html	A-ADO-INCO-061021/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user. User interaction is required to exploit this vulnerability. **CVE ID : CVE-2021-39819**		
indesign					
Out-of-bounds Read	29-Sep-21	6.8	Adobe InDesign versions 16.3 (and earlier), and 16.3.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious TIF file. **CVE ID : CVE-2021-39821**	https://helpx.adobe.com/security/products/indesign/apsb21-73.html	A-ADO-INDE-061021/13
photoshop_2020					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Sep-21	9.3	Adobe Photoshop versions 21.2.11 (and earlier) and 22.5 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-40709**	https://helpx.adobe.com/security/products/photoshop/apsb21-84.html	A-ADO-PHOT-061021/14
photoshop_2021					
Buffer Copy without	27-Sep-21	9.3	Adobe Photoshop versions 21.2.11 (and earlier) and 22.5	https://helpx.adobe.com	A-ADO-PHOT-061021/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			(and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-40709**	/security/products/photoshop/apsb21-84.html	
premiere_elements					
Access of Memory Location After End of Buffer	27-Sep-21	9.3	Adobe Premiere Elements version 2021.2235820 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious png file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. **CVE ID : CVE-2021-39824**	https://helpx.adobe.com/security/products/premiere_elements/apsb21-78.html	A-ADO-PREM-061021/16
adonisjs					
edge					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-21	5.8	This affects the package edge.js before 5.3.2. A type confusion vulnerability can be used to bypass input sanitization when the input to be rendered is an array (instead of a string or a SafeValue), even if {{ }} are	https://snyk.io/vuln/SNYK-JS-EDGEJS-1579556, https://github.com/edge-js/edge/commit/fa2c7fde86327aeae2	A-ADO-EDGE-061021/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used. **CVE ID : CVE-2021-23443**	32752e89a6e37e2e469e21	
Ait-pro					
bulletproof_security					
Exposure of Sensitive Information to an Unauthorized Actor	17-Sep-21	5	The BulletProof Security WordPress plugin is vulnerable to sensitive information disclosure due to a file path disclosure in the publicly accessible ~/db_backup_log.txt file which grants attackers the full path of the site, in addition to the path of database backup files. This affects versions up to, and including, 5.1. **CVE ID : CVE-2021-39327**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2591118%40bulletproof-security&new=2591118%40bulletproof-security&sfp_email=&sfph_mail=	A-AIT-BULL-061021/18
alojapro					
alojapro_widget					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The Alojapro Widget WordPress plugin through 1.1.15 doesn't properly sanitise its Custom CSS settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24530**	N/A	A-ALO-ALOJ-061021/19
Amazon					
aws_workspaces					
Improper Neutralizatio	22-Sep-21	9.3	In the Amazon AWS WorkSpaces client 3.0.10	https://docs.aws.amazon.	A-AMA-AWS_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Argument Delimiters in a Command ('Argument Injection')			through 3.1.8 on Windows, argument injection in the workspaces:// URI handler can lead to remote code execution because of the Chromium Embedded Framework (CEF) --gpu-launcher argument. This is fixed in 3.1.9. **CVE ID : CVE-2021-38112**	com/workspaces/latest/userguide/amazon-workspaces-windows-client.html#windows-release-notes	061021/20
ansi-regex_project					
ansi-regex					
N/A	17-Sep-21	7.8	ansi-regex is vulnerable to Inefficient Regular Expression Complexity **CVE ID : CVE-2021-3807**	https://github.com/chalk/ansi-regex/commit/8d1d7cdb586269882c4bdc1b7325d0c58c8f76f9, https://huntr.dev/bounties/5b3cf33b-ede0-4398-9974-800876dfd994	A-ANS-ANSI-061021/21
Apache					
druid					
Exposure of Resource to Wrong Sphere	24-Sep-21	4	In the Druid ingestion system, the InputSource is used for reading data from a certain data source. However, the HTTP InputSource allows authenticated users to read data from other sources than intended, such as the local file system, with the privileges of	https://lists.apache.org/thread.html/rc9400a70d0ec5cdb8a3486fc5ddb0b5282961c0b63e764abfbcb9f5d%40%3C	A-APA-DRUI-061021/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Druid server process. This is not an elevation of privilege when users access Druid directly, since Druid also provides the Local InputSource, which allows the same level of access. But it is problematic when users interact with Druid indirectly through an application that allows users to specify the HTTP InputSource, but not the Local InputSource. In this case, users could bypass the application-level restriction by passing a file URL to the HTTP InputSource. This issue was previously mentioned as being fixed in 0.21.0 as per CVE-2021-26920 but was not fixed in 0.21.1. **CVE ID : CVE-2021-36749**	dev.druid.apache.org%3E, https://lists.apache.org/thread.html/r304dfe56a5dfe1b2d9166b24d2c74ad1c6730338b20aef77a00ed2be@%3Cannounce.apache.org%3E	
http_server					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-21	7.5	ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier. **CVE ID : CVE-2021-39275**	https://httpd.apache.org/security/vulnerabilities_24.html, https://lists.apache.org/thread.html/r82c077663f9759c7df5a6656f925b3ee4f55fcd33c889ba7cd687029@%3Cusers.httpd.apache.org%3E	A-APA-HTTP-061021/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	16-Sep-21	7.5	A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier. **CVE ID : CVE-2021-40438**	https://httpd.apache.org/security/vulnerabilities_24.html, https://lists.apache.org/thread.html/r82c077663f9759c7df5a6656f925b3ee4f55fcd33c889ba7cd687029@%3Cusers.httpd.apache.org%3E	A-APA-HTTP-061021/24
NULL Pointer Dereference	16-Sep-21	5	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier. **CVE ID : CVE-2021-34798**	http://httpd.apache.org/security/vulnerabilities_24.html, https://lists.apache.org/thread.html/r82c077663f9759c7df5a6656f925b3ee4f55fcd33c889ba7cd687029@%3Cusers.httpd.apache.org%3E	A-APA-HTTP-061021/25
Out-of-bounds Read	16-Sep-21	5	A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).	http://httpd.apache.org/security/vulnerabilities_24.html, https://lists.apache.org/thread.html/r	A-APA-HTTP-061021/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36160	ee7519d71415ecdd170ff1889cab552d71758d2ba2904a17ded21a70@%3Ccvs.httpd.apache.org%3E	
jena					
Improper Restriction of XML External Entity Reference	16-Sep-21	5	A vulnerability in XML processing in Apache Jena, in versions up to 4.1.0, may allow an attacker to execute XML External Entities (XXE), including exposing the contents of local files to a remote server. **CVE ID : CVE-2021-39239**	https://lists.apache.org/thread.html/rf44d529c54ef1d0097e813f576a0823a727e1669a9f610d3221d493d%40%3Cusers.jena.apache.org%3E, https://lists.apache.org/thread.html/rf44d529c54ef1d0097e813f576a0823a727e1669a9f610d3221d493d@%3Cannounce.apache.org%3E	A-APA-JENA-061021/27
kafka					
Observable Discrepancy	22-Sep-21	4.3	Some components in Apache Kafka use `Arrays.equals` to validate a password or key, which is vulnerable to timing attacks that make brute force attacks for such credentials more likely to be successful.	https://kafka.apache.org/cve-list	A-APA-KAFK-061021/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Users should upgrade to 2.8.1 or higher, or 3.0.0 or higher where this vulnerability has been fixed. The affected versions include Apache Kafka 2.0.0, 2.0.1, 2.1.0, 2.1.1, 2.2.0, 2.2.1, 2.2.2, 2.3.0, 2.3.1, 2.4.0, 2.4.1, 2.5.0, 2.5.1, 2.6.0, 2.6.1, 2.6.2, 2.7.0, 2.7.1, and 2.8.0. **CVE ID : CVE-2021-38153**		
shiro					
Improper Authentication	17-Sep-21	7.5	Apache Shiro before 1.8.0, when using Apache Shiro with Spring Boot, a specially crafted HTTP request may cause an authentication bypass. Users should update to Apache Shiro 1.8.0. **CVE ID : CVE-2021-41303**	https://lists.apache.org/thread.html/re470be1ffea44bca28ccb0e67a4cf5d744e2d2b981d00fdbbf5abc13%40%3Cannounce.shiro.apache.org%3E	A-APA-SHIR-061021/29
tomcat					
Improper Input Validation	16-Sep-21	4.3	Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service. **CVE ID : CVE-2021-41079**	https://lists.apache.org/thread.html/rccdef0349fdf4fb73a4e4403095446d7fe6264e0a58e2df5c6799434%40%3Cannounce.tomcat.apache.org%3E	A-APA-TOMC-061021/30

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tomee					
Exposure of Sensitive Information to an Unauthorized Actor	19-Sep-21	5	All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfo from a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element. **CVE ID : CVE-2021-40690**	https://lists.apache.org/thread.html/r8848751b6a5dd78cc9e99d627e74fecfaffdfa1bb615dce827aad633%40%3Cdev.santuario.apache.org%3E, https://lists.apache.org/thread.html/rbdac116aef912b563da54f4c152222c0754e32fb2f785519ac5e059f@%3Ccommits.tomee.apache.org%3E	A-APA-TOME-061021/31
xml_security_for_java					
Exposure of Sensitive Information to an Unauthorized Actor	19-Sep-21	5	All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfo from a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.	https://lists.apache.org/thread.html/r8848751b6a5dd78cc9e99d627e74fecfaffdfa1bb615dce827aad633%40%3Cdev.santuario.apache.org%3E, https://lists.apache.org/t	A-APA-XML_-061021/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40690	hread.html/rbdac116aef912b563da54f4c152222c0754e32fb2f785519ac5e059f@%3Ccommits.tomee.apache.org%3E	
Asus					
armoury_crate_lite_service					
Uncontrolled Search Path Element	27-Sep-21	4.4	ASUS ROG Armoury Crate Lite before 4.2.10 allows local users to gain privileges by placing a Trojan horse file in the publicly writable %PROGRAMDATA%\ASUS\GamingCenterLib directory. **CVE ID : CVE-2021-40981**	N/A	A-ASU-ARMO-061021/33
Atlassian					
data_center					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Sep-21	6.5	Affected versions of Atlassian Jira Server or Data Center using the Jira Service Management addon allow remote attackers with JIRA Administrators access to execute arbitrary Java code via a server-side template injection vulnerability in the Email Template feature. The affected versions of Jira Server or Data Center are before version 8.13.12, and from version 8.14.0 before 8.19.1. **CVE ID : CVE-2021-39128**	N/A	A-ATL-DATA-061021/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jira					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Sep-21	6.5	Affected versions of Atlassian Jira Server or Data Center using the Jira Service Management addon allow remote attackers with JIRA Administrators access to execute arbitrary Java code via a server-side template injection vulnerability in the Email Template feature. The affected versions of Jira Server or Data Center are before version 8.13.12, and from version 8.14.0 before 8.19.1. **CVE ID : CVE-2021-39128**	N/A	A-ATL-JIRA-061021/35
aveva					
suitelink					
Heap-based Buffer Overflow	23-Sep-21	7.5	Heap-based buffer overflow in SuiteLink server while processing commands 0x05/0x06 **CVE ID : CVE-2021-32959**	https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2021-003.pdf	A-AVE-SUIT-061021/36
NULL Pointer Dereference	23-Sep-21	5	Null pointer dereference in SuiteLink server while processing commands 0x03/0x10 **CVE ID : CVE-2021-32963**	https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/Sec	A-AVE-SUIT-061021/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				urityBulletin_AVEVA-2021-003.pdf	
NULL Pointer Dereference	23-Sep-21	5	Null pointer dereference in SuiteLink server while processing command 0x07 **CVE ID : CVE-2021-32971**	https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2021-003.pdf	A-AVE-SUIT-061021/38
NULL Pointer Dereference	23-Sep-21	5	Null pointer dereference in SuiteLink server while processing commands 0x04/0x0a **CVE ID : CVE-2021-32979**	https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2021-003.pdf	A-AVE-SUIT-061021/39
NULL Pointer Dereference	23-Sep-21	5	Null pointer dereference in SuiteLink server while processing command 0x0b **CVE ID : CVE-2021-32987**	https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2021-003.pdf	A-AVE-SUIT-061021/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	23-Sep-21	5	Improper handling of exceptional conditions in SuiteLink server while processing command 0x01 **CVE ID : CVE-2021-32999**	https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2021-003.pdf	A-AVE-SUIT-061021/41
axiosys					
bento4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-21	6.8	An issue was discovered in Bento4 through v1.6.0-637. A global-buffer-overflow exists in the function AP4_MemoryByteStream::WritePartial() located in Ap4ByteStream.cpp. It allows an attacker to cause code execution or information disclosure. **CVE ID : CVE-2021-32265**	N/A	A-AXI-BENT-061021/42
Baidu					
ueditor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-21	3.5	Cross Site Scripting (XSS) vulnerability exists in UEditor v1.4.3.3, which can be exploited by an attacker to obtain user cookie information. **CVE ID : CVE-2021-37271**	N/A	A-BAI-UEDI-061021/43
zrender					
Improperly Controlled	17-Sep-21	7.5	ZRender is a lightweight graphic library providing 2d	https://github.com/ecomf	A-BAI-ZREN-061021/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Modification of Dynamically-Determined Object Attributes			draw for Apache ECharts. In versions prior to 5.2.1, using `merge` and `clone` helper methods in the `src/core/util.ts` module results in prototype pollution. It affects the popular data visualization library Apache ECharts, which uses and exports these two methods directly. The GitHub Security Advisory page for this vulnerability contains a proof of concept. This issue is patched in ZRender version 5.2.1. One workaround is available: Check if there is `__proto__` in the object keys. Omit it before using it as an parameter in these affected methods. Or in `echarts.util.merge` and `setOption` if project is using ECharts. **CVE ID : CVE-2021-39227**	e/zrender/security/advisories/GHSA-fhv8-fx5f-7fxf, https://github.com/ecomfe/zrender/pull/826	
bestiaweb					
gseor					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	A pageid GET parameter of the GSEOR â€“ WordPress SEO Plugin WordPress plugin through 1.3 is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. **CVE ID : CVE-2021-24396**	N/A	A-BES-GSEO-061021/45
boostnote					
boostnote					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Sep-21	7.5	static/main-preload.js in Boost Note through 0.22.0 allows remote command execution. A remote attacker may send a crafted IPC message to the exposed vulnerable ipcRenderer IPC interface, which invokes the dangerous openExternal Electron API. **CVE ID : CVE-2021-41392**	N/A	A-BOO-BOOS-061021/46
bootstrapped					
visual_link_preview					
Improper Access Control	20-Sep-21	5.5	The Visual Link Preview WordPress plugin before 2.2.3 does not enforce authorisation on several AJAX actions and has the CSRF nonce displayed for all authenticated users, allowing any authenticated user (such as subscriber) to call them and 1) Get and search through title and content of Draft post, 2) Get title of a password-protected post as well as 3) Upload an image from an URL **CVE ID : CVE-2021-24635**	N/A	A-BOO-VISU-061021/47
btcpayserver					
btcpay_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-Sep-21	3.5	btcpayserver is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3830**	https://huntr.dev/bounties/0fcdee5f-1f07-47ce-b650-ea8b4a7d35d8,	A-BTC-BTCP-061021/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')				https://github.com/btcpayserver/btcpayserver/commit/fc4e47cec608cc3dba24b19d0145ac69320b975e	
butter_project					
butter					
N/A	21-Sep-21	5	Butter is a system usability utility. Due to a kernel error the JPNS kernel is being discontinued. Affected users are recommend to update to the Trinity kernel. There are no workarounds. **CVE ID : CVE-2021-39230**	https://github.com/FrankEnderman/Butter/commit/a4fd717e848306f04f2823ea5f617e4da9f5bbdb, https://github.com/FrankEnderman/Butter/security/advisories/GHSA-4538-4g86-xf6j	A-BUT-BUTT-061021/49
bytecodealliance					
wasmtime					
Use After Free	17-Sep-21	3.3	Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing `externref`s from the host to guest Wasm content. To trigger the bug, you have to explicitly pass multiple	https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-v4cp-h94r-m7xf	A-BYT-WASM-061021/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			`externref`s from the host to a Wasm instance at the same time, either by passing multiple `externref`s as arguments from host code to a Wasm function, or returning multiple `externref`s to Wasm from a multi-value return function defined in the host. If you do not have host code that matches one of these shapes, then you are not impacted. If Wasmtime's `VMExternRefActivationsTable` became filled to capacity after passing the first `externref` in, then passing in the second `externref` could trigger a garbage collection. However the first `externref` is not rooted until we pass control to Wasm, and therefore could be reclaimed by the collector if nothing else was holding a reference to it or otherwise keeping it alive. Then, when control was passed to Wasm after the garbage collection, Wasm could use the first `externref`, which at this point has already been freed. We have reason to believe that the effective impact of this bug is relatively small because usage of `externref` is currently quite rare. The bug has been fixed, and users should upgrade to Wasmtime 0.30.0. If you cannot upgrade		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wasmtime yet, you can avoid the bug by disabling reference types support in Wasmtime by passing `false` to `wasmtime::Config::wasm_reference_types`. **CVE ID : CVE-2021-39216**		
Out-of-bounds Read	17-Sep-21	3.3	Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.26.0 and before version 0.30.0 is affected by a memory unsoundness vulnerability. There was an invalid free and out-of-bounds read and write bug when running Wasm that uses `externref`s in Wasmtime. To trigger this bug, Wasmtime needs to be running Wasm that uses `externref`s, the host creates non-null `externrefs`, Wasmtime performs a garbage collection (GC), and there has to be a Wasm frame on the stack that is at a GC safepoint where there are no live references at this safepoint, and there is a safepoint with live references earlier in this frame's function. Under this scenario, Wasmtime would incorrectly use the GC stack map for the safepoint from earlier in the function instead of the empty safepoint. This would result in Wasmtime treating	https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-4873-36h9-wv49, https://github.com/bytecodealliance/wasmtime/commit/398a73f0dd862dbe703212ebae8e34036a18c11c	A-BYT-WASM-061021/51

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary stack slots as `externref`s that needed to be rooted for GC. At the *next* GC, it would be determined that nothing was referencing these bogus `externref`s (because nothing could ever reference them, because they are not really `externref`s) and then Wasmtime would deallocate them and run `<ExternRef as Drop>::drop` on them. This results in a free of memory that is not necessarily on the heap (and shouldn't be freed at this moment even if it was), as well as potential out-of-bounds reads and writes. Even though support for `externref`s (via the reference types proposal) is enabled by default, unless you are creating non-null `externref`s in your host code or explicitly triggering GCs, you cannot be affected by this bug. We have reason to believe that the effective impact of this bug is relatively small because usage of `externref` is currently quite rare. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime at this time, you can avoid this bug by disabling the reference types proposal by passing `false` to `wasmtime::Config::wasm_ref		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			erence_types`. **CVE ID : CVE-2021-39218**		
Access of Resource Using Incompatible Type ('Type Confusion')	17-Sep-21	3.3	Wasmtime is an open source runtime for WebAssembly & WASI. Wasmtime before version 0.30.0 is affected by a type confusion vulnerability. As a Rust library the `wasmtime` crate clearly marks which functions are safe and which are `unsafe`, guaranteeing that if consumers never use `unsafe` then it should not be possible to have memory unsafety issues in their embeddings of Wasmtime. An issue was discovered in the safe API of `Linker::func_*` APIs. These APIs were previously not sound when one `Engine` was used to create the `Linker` and then a different `Engine` was used to create a `Store` and then the `Linker` was used to instantiate a module into that `Store`. Cross-`Engine` usage of functions is not supported in Wasmtime and this can result in type confusion of function pointers, resulting in being able to safely call a function with the wrong type. Triggering this bug requires using at least two `Engine` values in an embedding and then additionally using two different values with a `Linker` (one at the creation	https://github.com/bytecodealliance/wasmtime/commit/b39f087414f27ae40c44449ed5d1154e03449bff, https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-q879-9g95-56mx	A-BYT-WASM-061021/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			time of the `Linker` and another when instantiating a module with the `Linker`). It's expected that usage of more-than-one `Engine` in an embedding is relatively rare since an `Engine` is intended to be a globally shared resource, so the expectation is that the impact of this issue is relatively small. The fix implemented is to change this behavior to `panic!()` in Rust instead of silently allowing it. Using different `Engine` instances with a `Linker` is a programmer bug that `wasmtime` catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`. **CVE ID : CVE-2021-39219**		
Cisco					
embedded_wireless_controller					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP. **CVE ID : CVE-2021-1615**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ewc-dos-g6JruHRT	A-CIS-EMBE-061021/53
ios_xe					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	A-CIS-IOS_-061021/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**		
sd-wan					
Insufficiently Protected Credentials	23-Sep-21	3.5	A vulnerability in the disaster recovery feature of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to gain unauthorized access to user credentials. This vulnerability exists because access to API endpoints is not properly restricted. An attacker could exploit this vulnerability by sending a request to an API endpoint. A successful exploit could allow the attacker to gain unauthorized access to administrative credentials that could be used in further attacks. **CVE ID : CVE-2021-1589**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-credentials-ydYfskzZ	A-CIS-SD-W-061021/55
Improper Link Resolution Before File Access ('Link Following')	23-Sep-21	6.6	A vulnerability in the Cisco IOS XE SD-WAN Software CLI could allow an authenticated, local attacker to overwrite arbitrary files on the local system. This vulnerability is due to improper access controls on files within the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-GjR5pGOm	A-CIS-SD-W-061021/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system. A successful exploit could allow the attacker to overwrite arbitrary files on an affected device. **CVE ID : CVE-2021-1612**		
sd-wan_vbond_orchestrator					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	A-CIS-SD-W-061021/57
sd-wan_vmanage					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	A-CIS-SD-W-061021/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**		
wireless_lan_controller_software					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	A-CIS-WIRE-061021/59
client					
jointjs					
Access of Resource Using	21-Sep-21	7.5	This affects the package jointjs before 3.4.2. A type confusion vulnerability can	https://snyk.io/vuln/SNYK-JAVA-	A-CLI-JOIN-061021/60

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incompatible Type ('Type Confusion')			lead to a bypass of CVE-2020-28480 when the user-provided keys used in the path parameter are arrays in the setByPath function. **CVE ID : CVE-2021-23444**	ORGWEBJARSBOWER-1655817, https://github.com/clientIO/joint/releases/tag/v3.4.2, https://snyk.io/vuln/SNYK-JS-JOINTJS-1579578, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1655816, https://github.com/clientIO/joint/pull/1514	
cloudron					
cloudron					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-21	4.3	In Cloudron 6.2, the returnTo parameter on the login page is vulnerable to Reflected XSS. **CVE ID : CVE-2021-40868**	N/A	A-CLO-CLOU-061021/61
coder					
code-server					
N/A	17-Sep-21	7.8	code-server is vulnerable to Inefficient Regular Expression Complexity	https://huntr.dev/bounties/38888513-30fc-4d8f-	A-COD-CODE-061021/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-3810	805d-34070d60e223, https://github.com/cdr/code-server/commit/ca617df135e78833f93c8320cb2d2cf8bba809f5	
concretecms					
concrete_cms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Sep-21	6.5	An issue was discovered in Concrete CMS through 8.5.5. Authenticated path traversal leads to to remote code execution via uploaded PHP code, related to the bFilename parameter. **CVE ID : CVE-2021-40097**	https://documentation.concretecms.org/developers/introduction/version-history/856-release-notes	A-CON-CONC-061021/63
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Sep-21	7.5	An issue was discovered in Concrete CMS through 8.5.5. Path Traversal leading to RCE via external form by adding a regular expression. **CVE ID : CVE-2021-40098**	https://documentation.concretecms.org/developers/introduction/version-history/856-release-notes	A-CON-CONC-061021/64
N/A	24-Sep-21	6.5	An issue was discovered in Concrete CMS through 8.5.5. Fetching the update json scheme over HTTP leads to remote code execution. **CVE ID : CVE-2021-40099**	https://documentation.concretecms.org/developers/introduction/version-history/856-release-notes	A-CON-CONC-061021/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Sep-21	3.5	An issue was discovered in Concrete CMS through 8.5.5. Stored XSS can occur in Conversations when the Active Conversation Editor is set to Rich Text. **CVE ID : CVE-2021-40100**	https://documentation.concretecms.org/developers/introduction/version-history/856-release-notes	A-CON-CONC-061021/66
Deserialization of Untrusted Data	24-Sep-21	6.4	An issue was discovered in Concrete CMS through 8.5.5. Arbitrary File deletion can occur via PHAR deserialization in is_dir (PHP Object Injection associated with the __wakeup magic method). **CVE ID : CVE-2021-40102**	https://documentation.concretecms.org/developers/introduction/version-history/856-release-notes	A-CON-CONC-061021/67
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Sep-21	5	An issue was discovered in Concrete CMS through 8.5.5. Path Traversal can lead to Arbitrary File Reading and SSRF. **CVE ID : CVE-2021-40103**	https://documentation.concretecms.org/developers/introduction/version-history/856-release-notes	A-CON-CONC-061021/68
Incorrect Authorization	27-Sep-21	5	An issue was discovered in Concrete CMS through 8.5.5. There is an SVG sanitizer bypass. **CVE ID : CVE-2021-40104**	https://documentation.concretecms.org/developers/introduction/version-history/856-release-notes	A-CON-CONC-061021/69
Improper Neutralization of Input During Web Page Generation	27-Sep-21	4.3	An issue was discovered in Concrete CMS through 8.5.5. There is XSS via Markdown Comments. **CVE ID : CVE-2021-40105**	https://documentation.concretecms.org/developers/introduction/version-	A-CON-CONC-061021/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				history/856-release-notes	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	4.3	An issue was discovered in Concrete CMS through 8.5.5. There is unauthenticated stored XSS in blog comments via the website field. **CVE ID : CVE-2021-40106**	https://documentation.concretecms.org/developers/introduction/version-history/856-release-notes	A-CON-CONC-061021/71
Cross-Site Request Forgery (CSRF)	27-Sep-21	6.8	An issue was discovered in Concrete CMS through 8.5.5. The Calendar is vulnerable to CSRF. ccm_token is not verified on the ccm/calendar/dialogs/event/add/save endpoint. **CVE ID : CVE-2021-40108**	https://documentation.concretecms.org/developers/introduction/version-history/856-release-notes	A-CON-CONC-061021/72
Server-Side Request Forgery (SSRF)	27-Sep-21	5.5	A SSRF issue was discovered in Concrete CMS through 8.5.5. Users can access forbidden files on their local network. A user with permissions to upload files from external sites can upload a URL that redirects to an internal resource of any file type. The redirect is followed and loads the contents of the file from the redirected-to server. Files of disallowed types can be uploaded. **CVE ID : CVE-2021-40109**	https://documentation.concretecms.org/developers/introduction/version-history/856-release-notes	A-CON-CONC-061021/73
Cross-Site Request Forgery (CSRF)	23-Sep-21	5.8	A CSRF in Concrete CMS version 8.5.5 and below allows an attacker to duplicate files which can lead to UI inconvenience, and	N/A	A-CON-CONC-061021/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exhaustion of disk space.Credit for discovery: "Solar Security CMS Research Team" **CVE ID : CVE-2021-22949**		
Cross-Site Request Forgery (CSRF)	23-Sep-21	4.3	Concrete CMS prior to 8.5.6 had a CSFR vulnerability allowing attachments to comments in the conversation section to be deleted.Credit for discovery: "Solar Security Research Team" **CVE ID : CVE-2021-22950**	N/A	A-CON-CONC-061021/75
Cross-Site Request Forgery (CSRF)	23-Sep-21	5.8	A CSRF in Concrete CMS version 8.5.5 and below allows an attacker to clone topics which can lead to UI inconvenience, and exhaustion of disk space.Credit for discovery: "Solar Security Research Team" **CVE ID : CVE-2021-22953**	N/A	A-CON-CONC-061021/76
cookiex-deep_project					
cookiex-deep					
Improperly Controlled Modification of Dynamically-Determined Object Attributes	17-Sep-21	7.5	This affects all versions of package @cookiex/deep. The global proto object can be polluted using the __proto__ object. **CVE ID : CVE-2021-23442**	https://github.com/tony-tsx/cookiex-deep/issues/1, https://snyk.io/vuln/SNYK-JS-COOKIEXDEEP-1582793, https://github.com/tony-	A-COO-COOK-061021/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				tsx/cookiex-deep/commit/b5bea2b7f34a5fa9abb4446cbd038ecdbcd09c88	
couchbase					
couchbase_server					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Sep-21	5	Couchbase Server 6.5.x, 6.6.x through 6.6.2, and 7.0.0 has a Buffer Overflow. A specially crafted network packet sent from an attacker can crash memcached. **CVE ID : CVE-2021-35944**	https://www.couchbase.com/alerts, https://docs.couchbase.com/server/current/release-notes/relnotes.html	A-COU-COUC-061021/78
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Sep-21	5	Couchbase Server 6.5.x, 6.6.0 through 6.6.2, and 7.0.0, has a Buffer Overflow. A specially crafted network packet sent from an attacker can crash memcached. **CVE ID : CVE-2021-35945**	https://www.couchbase.com/alerts, https://docs.couchbase.com/server/current/release-notes/relnotes.html	A-COU-COUC-061021/79
creolabs					
gravity					
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in gravity through 0.8.1. A heap-buffer-overflow exists in the function gnode_function_add_upvalue located in gravity_ast.c. It allows an attacker to cause code Execution.	N/A	A-CRE-GRAV-061021/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-32281		
Out-of-bounds Write	20-Sep-21	4.3	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function ircode_add_check() located in gravity_ircode.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-32282**	N/A	A-CRE-GRAV-061021/81
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function gravity_string_to_value() located in gravity_value.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-32283**	N/A	A-CRE-GRAV-061021/82
NULL Pointer Dereference	20-Sep-21	6.8	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function ircode_register_pop_context_protect() located in gravity_ircode.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-32284**	N/A	A-CRE-GRAV-061021/83
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function list_iterator_next() located in gravity_core.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-32285**	N/A	A-CRE-GRAV-061021/84

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cusmin					
absolutely_glamorous_custom_admin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	Authenticated Stored Cross-Site Scripting (XSS) vulnerability in WordPress Absolutely Glamorous Custom Admin plugin (versions <= 6.8). Stored XSS possible via unsanitized input fields of the plugin settings, some of the payloads could make the frontend and the backend inaccessible. **CVE ID : CVE-2021-36823**	https://plugins.svn.wordpress.org/ag-custom-admin/trunk/changelog.txt	A-CUS-ABSO-061021/85
Dadamailproject					
dada_mail					
Cross-Site Request Forgery (CSRF)	20-Sep-21	6.8	Dada Mail is a web-based e-mail list management system. In affected versions a bad actor could give someone a carefully crafted web page via email, SMS, etc, that - when visited, allows them control of the list control panel as if the bad actor was logged in themselves. This includes changing any mailing list password, as well as the Dada Mail Root Password - which could effectively shut out actual list owners of the mailing list and allow the bad actor complete and unfettered control of your mailing list. This vulnerability also affects profile logins. For this vulnerability to work, the target of the bad actor would need to be logged into the list	https://github.com/justingit/dada-mail/commit/d4d3d86d08c816b4da75a5ef45abc12188772459, https://github.com/justingit/dada-mail/security/advisories/GHSA-344m-p829-2r38	A-DAD-DADA-061021/86

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			control panel themselves. This CSRF vulnerability in Dada Mail affects all versions of Dada Mail v11.15.1 and below. Although we know of no known CSRF exploits that have happened in the wild, this vulnerability has been confirmed by our testing, and by a third party. Users are advised to update to version 11.16.0. **CVE ID : CVE-2021-41083**		
Datev					
framework_library					
Incorrect Permission Assignment for Critical Resource	23-Sep-21	7.5	Insecure permissions in Update Manager <= 5.8.0.2300 and DFL <= 12.5.1001.5 in DATEV programs v14.1 allows attacker to escalate privileges via insufficient configuration of service components. **CVE ID : CVE-2021-41428**	https://apps.datev.de/help-center/documents/1021197	A-DAT-FRAM-061021/87
program					
Incorrect Permission Assignment for Critical Resource	23-Sep-21	7.5	Insecure permissions in Update Manager <= 5.8.0.2300 and DFL <= 12.5.1001.5 in DATEV programs v14.1 allows attacker to escalate privileges via insufficient configuration of service components. **CVE ID : CVE-2021-41428**	https://apps.datev.de/help-center/documents/1021197	A-DAT-PROG-061021/88
update_manager					
Incorrect Permission Assignment	23-Sep-21	7.5	Insecure permissions in Update Manager <= 5.8.0.2300 and DFL <=	https://apps.datev.de/help-	A-DAT-UPDA-061021/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
for Critical Resource			12.5.1001.5 in DATEV programs v14.1 allows attacker to escalate privileges via insufficient configuration of service components. **CVE ID : CVE-2021-41428**	center/documents/1021197	
Dell					
emc_networker					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-21	4	Dell NetWorker, versions 18.x and 19.x contain a Path traversal vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and gain access to unauthorized information. **CVE ID : CVE-2021-21569**	https://www.dell.com/support/kbdoc/en-us/000188311/	A-DEL-EMC_-061021/90
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Sep-21	4	Dell NetWorker, versions 18.x and 19.x contain an Information disclosure vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and gain access to unauthorized information. **CVE ID : CVE-2021-21570**	https://www.dell.com/support/kbdoc/en-us/000188311/dsa-2021-124-dell-networker-security-update-for-multiple-vulnerabilities	A-DEL-EMC_-061021/91
supportassist_client_consumer					
Improper Limitation of a Pathname to a Restricted	28-Sep-21	3.6	Dell SupportAssist Client Consumer versions 3.9.13.0 and any versions prior to 3.9.13.0 contain an arbitrary file deletion vulnerability that	https://www.dell.com/support/kbdoc/en-us/0001910	A-DEL-SUPP-061021/92

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			can be exploited by using the Windows feature of NTFS called Symbolic links. Symbolic links can be created by any(non-privileged) user under some object directories, but by themselves are not sufficient to successfully escalate privileges. However, combining them with a different object, such as the NTFS junction point allows for the exploitation. Support assist clean files functionality do not distinguish junction points from the physical folder and proceeds to clean the target of the junction that allows nonprivileged users to create junction points and delete arbitrary files on the system which can be accessed only by the admin. **CVE ID : CVE-2021-36286**	57/dsa-2021-163-dell-supportassist-client-consumer-security-update-for-two-vulnerabilities	
device42					
device42					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	17-Sep-21	8.5	The Device42 Main Appliance before 17.05.01 does not sanitize user input in its Nmap Discovery utility. An attacker (with permissions to add or edit jobs run by this utility) can inject an extra argument to overwrite arbitrary files as the root user on the Remote Collector. **CVE ID : CVE-2021-41316**	https://docs.device42.com/auto-discovery/nmap-autodiscovery/, https://blog.device42.com/2021/09/critical-fixes-in-17-05-01/,	A-DEV-DEVI-061021/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://docs.device42.com/auto-discovery/remote-collector-rc/	
remote_collector					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Sep-21	9	The Device42 Remote Collector before 17.05.01 does not sanitize user input in its SNMP Connectivity utility. This allows an authenticated attacker (with access to the console application) to execute arbitrary OS commands and escalate privileges. **CVE ID : CVE-2021-41315**	https://blog.device42.com/2021/09/critical-fixes-in-17-05-01/, https://docs.device42.com/auto-discovery/remote-collector-rc/	A-DEV-REMO-061021/94
dfactory					
post_views_counter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The Post Views Counter WordPress plugin before 1.3.5 does not sanitise or escape its Post Views Label settings, which could allow high privilege users to perform Cross-Site Scripting attacks in the frontend even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24613**	N/A	A-DFA-POST-061021/95
display_users_project					
display_users					
Improper Neutralization of Special Elements	20-Sep-21	6.5	The Edit Role functionality in the Display Users WordPress plugin through 2.0.0 had an `id` parameter which is not	N/A	A-DIS-DISP-061021/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. **CVE ID : CVE-2021-24400**		
dpl					
product_feed_on_woocommerce					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The fetch_product_ajax functionality in the Product Feed on WooCommerce WordPress plugin before 3.3.1.0 uses a `product_id` POST parameter which is not properly sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. **CVE ID : CVE-2021-24511**	https://codevigilant.com/disclosure/2021/wp-plugin-purple-xmls-google-product-feed-for-woocommerce/	A-DPL-PROD-061021/97
Ec-cube					
ec-cube					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-21	4.3	Cross-site scripting vulnerability in List (order management) item change plug-in (for EC-CUBE 3.0 series) Ver.1.1 and earlier allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20825**	N/A	A-EC--EC-C-061021/98
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-21	4.3	Cross-site scripting vulnerability in Order Status Batch Change Plug-in (for EC-CUBE 3.0 series) all versions allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20828**	N/A	A-EC--EC-C-061021/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
eideasy					
eid_easy					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	4.3	The eID Easy WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the error parameter found in the ~/admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 4.6. **CVE ID : CVE-2021-34650**	https://plugins.trac.wordpress.org/browser/smart-id/trunk/admin.php?rev=2451347#L30	A-EID-EID_-061021/100
elv					
elvish					
Exposure of Resource to Wrong Sphere	23-Sep-21	9.3	Elvish is a programming language and interactive shell, combined into one package. In versions prior to 0.14.0 Elvish's web UI backend (started by `elvish -web`) hosts an endpoint that allows executing the code sent from the web UI. The backend does not check the origin of requests correctly. As a result, if the user has the web UI backend open and visits a compromised or malicious website, the website can send arbitrary code to the endpoint in localhost. All Elvish releases from 0.14.0 onward no longer include the the web UI, although it is still possible for the user to build a version from source that includes the web UI. The issue can be patched for previous versions	https://github.com/elves/elvish/security/advisories/GHSA-fpv6-f8jw-rc3r, https://github.com/elves/elvish/commit/ccc2750037bbbfafe9c1b7a78eadd3bd16e81fe5	A-ELV-ELVI-061021/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by removing the web UI (found in web, pkg/web or pkg/prog/web, depending on the exact version). **CVE ID : CVE-2021-41088**		
enbra					
ewm					
Use of Hard-coded Credentials	16-Sep-21	2.9	Multiple Wireless M-Bus devices by Enbra use Hard-coded Credentials in Security mode 5 without an option to change the encryption key. An adversary can learn all information that is available in Enbra EWM. **CVE ID : CVE-2021-34571**	https://www.fit.vutbr.cz/~polcak/CVE-2021-34571.en	A-ENB-EWM-061021/102
Insufficient Verification of Data Authenticity	16-Sep-21	3.3	Enbra EWM 1.7.29 does not check for or detect replay attacks sent by wireless M-Bus Security mode 5 devices. Instead timestamps of the sensor are replaced by the time of the readout even if the data is a replay of earlier data. **CVE ID : CVE-2021-34572**	https://www.fit.vutbr.cz/~polcak/CVE-2021-34572.en	A-ENB-EWM-061021/103
Incorrect Calculation	16-Sep-21	2.1	In Enbra EWM in Version 1.7.29 together with several tested wireless M-Bus Sensors the events backflow and "no flow" are not reconized or misinterpreted. This may lead to wrong values and missing events. **CVE ID : CVE-2021-34573**	https://www.fit.vutbr.cz/~polcak/CVE-2021-34573.en	A-ENB-EWM-061021/104
Ericsson					
enterprise_content_management					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Sep-21	6	In Ericsson ECM before 18.0, it was observed that Security Provider Endpoint in the User Profile Management Section is vulnerable to CSV Injection. **CVE ID : CVE-2021-41390**	N/A	A-ERI-ENTE-061021/105
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-21	3.5	In Ericsson ECM before 18.0, it was observed that Security Management Endpoint in User Profile Management Section is vulnerable to stored XSS via a name, leading to session hijacking and full account takeover. **CVE ID : CVE-2021-41391**	N/A	A-ERI-ENTE-061021/106
faad2_project					
faad2					
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in faad2 before 2.10.0. A heap-buffer-overflow exists in the function stszin located in mp4read.c. It allows an attacker to cause Code Execution. **CVE ID : CVE-2021-32272**	https://github.com/knik0/faad2/commit/1b71a6ba963d131375f5e489b3b25e36f19f3f24	A-FAA-FAAD-061021/107
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in faad2 through 2.10.0. A stack-buffer-overflow exists in the function ftypin located in mp4read.c. It allows an attacker to cause Code Execution. **CVE ID : CVE-2021-32273**	N/A	A-FAA-FAAD-061021/108
Out-of-bounds	20-Sep-21	6.8	An issue was discovered in faad2 through 2.10.0. A heap-	N/A	A-FAA-FAAD-061021/109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			buffer-overflow exists in the function sbr_qmf_synthesis_64 located in sbr_qmf.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-32274**		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in faad2 through 2.10.0. A NULL pointer dereference exists in the function get_sample() located in output.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-32276**	N/A	A-FAA-FAAD-061021/110
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function sbr_qmf_analysis_32 located in sbr_qmf.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-32277**	N/A	A-FAA-FAAD-061021/111
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function lt_prediction located in lt_predict.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-32278**	N/A	A-FAA-FAAD-061021/112
Ffmpeg					
ffmpeg					
Integer Overflow or Wraparound	20-Sep-21	6.8	Integer Overflow vulnerability in function filter16_roberts in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows	https://git.ffmpeg.org/gitweb/ffmpeg.git/commit/99f8d32129	A-FFM-FFMP-061021/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a Denial of Service or other unspecified impacts. **CVE ID : CVE-2021-38090**	dd233d4eb2efa44678a0bc44869f23, https://trac.ffmpeg.org/ticket/8263	
Integer Overflow or Wraparound	20-Sep-21	6.8	Integer Overflow vulnerability in function filter16_sobel in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts. **CVE ID : CVE-2021-38091**	https://git.ffmpeg.org/gitweb/ffmpeg.git/commit/99f8d32129dd233d4eb2efa44678a0bc44869f23, https://trac.ffmpeg.org/ticket/8263	A-FFM-FFMP-061021/114
Integer Overflow or Wraparound	20-Sep-21	6.8	Integer Overflow vulnerability in function filter_prewitt in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts. **CVE ID : CVE-2021-38092**	https://git.ffmpeg.org/gitweb/ffmpeg.git/commit/99f8d32129dd233d4eb2efa44678a0bc44869f23, https://trac.ffmpeg.org/ticket/8263	A-FFM-FFMP-061021/115
Integer Overflow or Wraparound	20-Sep-21	6.8	Integer Overflow vulnerability in function filter_robert in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts. **CVE ID : CVE-2021-38093**	https://git.ffmpeg.org/gitweb/ffmpeg.git/commit/99f8d32129dd233d4eb2efa44678a0bc44869f23, https://trac.ffmpeg.org/ticket/8263	A-FFM-FFMP-061021/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	20-Sep-21	6.8	Integer Overflow vulnerability in function filter_sobel in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts. **CVE ID : CVE-2021-38094**	https://git.ffmpeg.org/gitweb/ffmpeg.git/commit/99f8d32129dd233d4eb2efa44678a0bc44869f23, https://trac.ffmpeg.org/ticket/8263	A-FFM-FFMP-061021/117
ffw					
omgf					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Sep-21	6.4	The OMGF WordPress plugin before 4.5.4 does not escape or validate the handle parameter of the REST API, which allows unauthenticated users to perform path traversal and overwrite arbitrary CSS file with Google Fonts CSS, or download fonts uploaded on Google Fonts website. **CVE ID : CVE-2021-24638**	N/A	A-FFW-OMGF-061021/118
Cross-Site Request Forgery (CSRF)	20-Sep-21	5.5	The OMGF WordPress plugin before 4.5.4 does not enforce path validation, authorisation and CSRF checks in the omgf_ajax_empty_dir AJAX action, which allows any authenticated users to delete arbitrary files or folders on the server. **CVE ID : CVE-2021-24639**	N/A	A-FFW-OMGF-061021/119
firefly-iii					
firefly_iii					
Cross-Site	27-Sep-21	6.8	firefly-iii is vulnerable to	https://hunt	A-FIR-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2021-3819**	r.dev/bounties/da82f7b6-4ffc-4109-87a4-a2a790bd44e5, https://github.com/firefly-iii/firefly-iii/commit/578f350498b75f31d321c78a608c7f7b3b7b07e9	061021/120
flask-restx_project					
flask-restx					
Uncontrolled Resource Consumption	20-Sep-21	5	Flask-RESTX (pypi package flask-restx) is a community driven fork of Flask-RESTPlus. Flask-RESTX before version 0.5.1 is vulnerable to ReDoS (Regular Expression Denial of Service) in email_regex. This is fixed in version 0.5.1. **CVE ID : CVE-2021-32838**	https://github.com/python-restx/flask-restx/issues/372, https://github.com/python-restx/flask-restx/commit/bab31e085f355dd73858fd3715f7ed71849656da, https://github.com/advisories/GHSA-3q6g-vf58-7m4g	A-FLA-FLAS-061021/121
fontsplugin					
fonts					
Improper	20-Sep-21	3.5	The Google Fonts	N/A	A-FON-FONT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Typography WordPress plugin before 3.0.3 does not escape and sanitise some of its block settings, allowing users with as role as low as Contributor to perform Stored Cross-Site Scripting attacks via blockType (combined with content), align, color, variant and fontID argument of a Gutenberg block. **CVE ID : CVE-2021-24637**		061021/122
frogcms_project					
frogcms					
Unrestricted Upload of File with Dangerous Type	23-Sep-21	7.5	Privilege escalation in 'upload.php' in FrogCMS SentCMS v0.9.5 allows attacker to execute arbitrary code via crafted php file. **CVE ID : CVE-2021-26794**	N/A	A-FRO-FROG-061021/123
getgrav					
grav					
Reliance on Cookies without Validation and Integrity Checking	27-Sep-21	5	grav is vulnerable to Reliance on Cookies without Validation and Integrity Checking **CVE ID : CVE-2021-3818**	https://huntr.dev/bounties/c2bc65af-7b93-4020-886e-8cdaeb0a58ea	A-GET-GRAV-061021/124
grav-plugin-admin					
Improper Restriction of Rendered UI Layers or Frames	27-Sep-21	5.8	grav-plugin-admin is vulnerable to Improper Restriction of Rendered UI Layers or Frames **CVE ID : CVE-2021-3799**	https://huntr.dev/bounties/d73f24a8-302b-4f9f-abb8-54688abd9813,	A-GET-GRAV-061021/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://github.com/getgrav/grav-plugin-admin/commit/853abfbbd3c14a0a601c941dcfaa3858b6283b69	
getshortcodes					
shortcodes_ultimate					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The Shortcodes Ultimate WordPress plugin before 5.10.2 allows users with Contributor roles to perform stored XSS via shortcode attributes. Note: the plugin is inconsistent in its handling of shortcode attributes; some do escape, most don't, and there are even some attributes that are insecure by design (like [su_button]'s onclick attribute). **CVE ID : CVE-2021-24525**	N/A	A-GET-SHOR-061021/126
Github					
enterprise_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Sep-21	4	A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server	https://docs.github.com/en/enterprise-server@3.1/admin/release-notes#3.1.8, https://docs.github.com/en/enterprise	A-GIT-ENTE-061021/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.8 and was fixed in 3.1.8, 3.0.16, and 2.22.22. This vulnerability was reported via the GitHub Bug Bounty program. This is the result of an incomplete fix for CVE-2021-22867. **CVE ID : CVE-2021-22868**	-server@3.0/admin/release-notes#3.0.16, https://docs.github.com/en/enterprise-server@2.22/admin/release-notes#2.22.22	
Exposure of Resource to Wrong Sphere	24-Sep-21	7.5	An improper access control vulnerability in GitHub Enterprise Server allowed a workflow job to execute in a self-hosted runner group it should not have had access to. This affects customers using self-hosted runner groups for access control. A repository with access to one enterprise runner group could access all of the enterprise runner groups within the organization because of improper authentication checks during the request. This could cause code to be run unintentionally by the incorrect runner group. This vulnerability affected GitHub Enterprise Server versions from 3.0.0 to 3.0.15 and 3.1.0 to 3.1.7 and was fixed in	https://docs.github.com/en/enterprise-server@3.1/admin/release-notes#3.1.8, https://docs.github.com/en/enterprise-server@3.0/admin/release-notes#3.0.16	A-GIT-ENTE-061021/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.0.16 and 3.1.8 releases. **CVE ID : CVE-2021-22869**		
GNU					
libredwg					
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function bit_read_BB() located in bits.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39521**	https://github.com/LibreDWG/libredwg/issues/262	A-GNU-LIBR-061021/129
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in libredwg through v0.10.1.3751. bit_wcs2len() in bits.c has a heap-based buffer overflow. **CVE ID : CVE-2021-39522**	https://github.com/LibreDWG/libredwg/issues/255	A-GNU-LIBR-061021/130
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function check_POLYLINE_handles() located in decode.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39523**	N/A	A-GNU-LIBR-061021/131
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in libredwg through v0.10.1.3751. bit_read_fixed() in bits.c has a heap-based buffer overflow. **CVE ID : CVE-2021-39525**	N/A	A-GNU-LIBR-061021/132
Out-of-bounds	20-Sep-21	6.8	An issue was discovered in libredwg through	N/A	A-GNU-LIBR-061021/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			v0.10.1.3751. appinfo_private() in decode.c has a heap-based buffer overflow. **CVE ID : CVE-2021-39527**		
Double Free	20-Sep-21	6.8	An issue was discovered in libredwg through v0.10.1.3751. dwg_free_MATERIAL_private() in dwg.spec has a double free. **CVE ID : CVE-2021-39528**	https://github.com/LibreDWG/libredwg/issues/256	A-GNU-LIBR-061021/134
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in libredwg through v0.10.1.3751. bit_wcs2nlen() in bits.c has a heap-based buffer overflow. **CVE ID : CVE-2021-39530**	https://github.com/LibreDWG/libredwg/issues/258	A-GNU-LIBR-061021/135
ncurses					
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in ncurses through v6.2-1. _nc_captoinfo in captoinfo.c has a heap-based buffer overflow. **CVE ID : CVE-2021-39537**	https://lists.gnu.org/archive/html/bug-ncurses/2020-08/msg00006.html	A-GNU-NCUR-061021/136
goteleport					
teleport					
Improper Authentication	18-Sep-21	7.5	Teleport before 4.4.11, 5.x before 5.2.4, 6.x before 6.2.12, and 7.x before 7.1.1 allows forgery of SSH host certificates in some situations. **CVE ID : CVE-2021-41393**	https://github.com/gravitational/teleport/releases/tag/v6.2.12, https://github.com/gravitational/teleport/releases/	A-GOT-TELE-061021/137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				tag/v4.4.11, https://github.com/gravitational/teleport/releases/tag/v5.2.4, https://github.com/gravitational/teleport/releases/tag/v7.1.1	
N/A	18-Sep-21	5	Teleport before 4.4.11, 5.x before 5.2.4, 6.x before 6.2.12, and 7.x before 7.1.1 allows alteration of build artifacts in some situations. **CVE ID : CVE-2021-41394**	https://github.com/gravitational/teleport/releases/tag/v6.2.12, https://github.com/gravitational/teleport/releases/tag/v4.4.11, https://github.com/gravitational/teleport/releases/tag/v5.2.4, https://github.com/gravitational/teleport/releases/tag/v7.1.1	A-GOT-TELE-061021/138
N/A	18-Sep-21	6.4	Teleport before 6.2.12 and 7.x before 7.1.1 allows attackers to control a database connection string, in some situations, via a crafted database name or username. **CVE ID : CVE-2021-41395**	https://github.com/gravitational/teleport/releases/tag/v6.2.12, https://github.com/gravitational/teleport/releases/	A-GOT-TELE-061021/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				tag/v7.1.1	
gpac					
gpac					
Out-of-bounds Write	20-Sep-21	6.8	Buffer overflow vulnerability in function gf_fprintf in os_file.c in gpac before 1.0.1 allows attackers to execute arbitrary code. The fixed version is 1.0.1. **CVE ID : CVE-2021-32268**	https://github.com/gpac/gpac/issues/1587	A-GPA-GPAC-061021/140
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in gpac through 20200801. A NULL pointer dereference exists in the function ilst_item_box_dump located in box_dump.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-32269**	N/A	A-GPA-GPAC-061021/141
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in gpac through 20200801. A NULL pointer dereference exists in the function vwid_box_del located in box_code_base.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-32270**	N/A	A-GPA-GPAC-061021/142
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in gpac through 20200801. A stack-buffer-overflow exists in the function DumpRawUIConfig located in odf_dump.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-32271**	N/A	A-GPA-GPAC-061021/143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Gradle					
gradle					
Exposure of Sensitive Information to an Unauthorized Actor	24-Sep-21	5	Gradle Enterprise before 2021.1.3 can allow unauthorized viewing of a response (information disclosure of possibly sensitive build/configuration details) via a crafted HTTP request with the X-Gradle-Enterprise-Ajax-Request header. **CVE ID : CVE-2021-41584**	https://security.gradle.com/advisory/2021-02	A-GRA-GRAD-061021/144
Server-Side Request Forgery (SSRF)	24-Sep-21	5	In Gradle Enterprise before 2021.1.3, an attacker with the ability to perform SSRF attacks can potentially reset the system user password. **CVE ID : CVE-2021-41586**	https://security.gradle.com/advisory/2021-05	A-GRA-GRAD-061021/145
Server-Side Request Forgery (SSRF)	24-Sep-21	5	In Gradle Enterprise before 2021.1.3, an attacker with the ability to perform SSRF attacks can potentially discover credentials for other resources. **CVE ID : CVE-2021-41587**	https://security.gradle.com/advisory/2021-04	A-GRA-GRAD-061021/146
Deserialization of Untrusted Data	24-Sep-21	6.8	In Gradle Enterprise before 2021.1.3, a crafted request can trigger deserialization of arbitrary unsafe Java objects. The attacker must have the encryption and signing keys. **CVE ID : CVE-2021-41588**	https://security.gradle.com/advisory/2021-03	A-GRA-GRAD-061021/147
grame					
faust					
NULL Pointer	20-Sep-21	4.3	An issue was discovered in faust through v2.30.5. A NULL	N/A	A-GRA-FAUS-061021/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			pointer dereference exists in the function CosPrim::computeSigOutput( ) located in cosprim.hh. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-32275**		
Gurock					
testrail					
Incorrect Authorizatio n	22-Sep-21	5	Improper Access Control in Gurock TestRail versions < 7.2.0.3014 resulted in sensitive information exposure. A threat actor can access the /files.md5 file on the client side of a Gurock TestRail application, disclosing a full list of application files and the corresponding file paths. The corresponding file paths can be tested, and in some cases, result in the disclosure of hardcoded credentials, API keys, or other sensitive data. **CVE ID : CVE-2021-40875**	https://ww w.gurock.co m/testrail/to ur/enterpris e-edition	A-GUR-TEST-061021/149
gutenslider					
gutenslider					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The WordPress Slider Block Gutenslider plugin before 5.2.0 does not escape the minWidth attribute of a Gutenburg block, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks **CVE ID : CVE-2021-24640**	N/A	A-GUT-GUTE-061021/150
hcxtools_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
hcxtoold					
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in hcxtools through 6.1.6. A global-buffer-overflow exists in the function pcapngoptionwalk located in hcxpcapngtool.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-32286**	https://github.com/ZerBea/hcxtools/issues/155	A-HCX-HCXT-061021/151
IBM					
aspera_on_cloud					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Aspera Cloud is vulnerable to stored 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: 208343. **CVE ID : CVE-2021-38870**	https://www.ibm.com/support/pages/node/6491603, https://exchange.xforce.ibmcloud.com/vulnerabilities/208343	A-IBM-ASPE-061021/152
business_automation_workflow					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Sep-21	3.5	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3,20.0.0.1, 20.0.0.2, and 21.0.2 and IBM Business Process Manager 8.5 and 8.6 are vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	https://www.ibm.com/support/pages/node/6493271, https://exchange.xforce.ibmcloud.com/vulnerabilities/204832	A-IBM-BUSI-061021/153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204832. **CVE ID : CVE-2021-29834**		
business_process_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Sep-21	3.5	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3,20.0.0.1, 20.0.0.2, and 21.0.2 and IBM Business Process Manager 8.5 and 8.6 are vulnerable to stored 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: 204832. **CVE ID : CVE-2021-29834**	https://www.ibm.com/support/pages/node/6493271, https://exchange.xforce.ibmcloud.com/vulnerabilities/204832	A-IBM-BUSI-061021/154
cloud_pak_for_data					
Exposure of Sensitive Information to an Unauthorized Actor	20-Sep-21	2.1	IBM Cloud Pak for Data 2.5 could allow a local user with special privileges to obtain highly sensitive information. IBM X-Force ID: 209575. **CVE ID : CVE-2021-38899**	https://www.ibm.com/support/pages/node/6490435	A-IBM-CLOU-061021/155
db2					
Exposure of Sensitive Information to an Unauthorize	16-Sep-21	3.5	IBM Db2 11.2 and 11.5 contains an information disclosure vulnerability, exposing remote storage credentials to privileged	https://www.ibm.com/support/pages/node/6489489,	A-IBM-DB2-061021/156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Actor			users under specific conditions. IBM X-Fporce ID: 201780. **CVE ID : CVE-2021-29752**	https://exchange.xforce.ibmcloud.com/vulnerabilities/201780	
Allocation of Resources Without Limits or Throttling	16-Sep-21	1.9	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267. **CVE ID : CVE-2021-29763**	https://www.ibm.com/support/pages/node/6489493, https://exchange.xforce.ibmcloud.com/vulnerabilities/202267	A-IBM-DB2-061021/157
Exposure of Sensitive Information to an Unauthorized Actor	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470. **CVE ID : CVE-2021-29825**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204470, https://www.ibm.com/support/pages/node/6489499	A-IBM-DB2-061021/158
jazz_for_service_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored 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	https://exchange.xforce.ibmcloud.com/vulnerabilities/208405, https://www.ibm.com/support/pages/node/6491521	A-IBM-JAZZ-061021/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session. IBM X-Force ID: 208405. **CVE ID : CVE-2021-38877**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Tivoli Netcool/OMNIbus_GUI and IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored 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-2021-29800**	https://www.ibm.com/support/pages/node/6491109, https://exchange.xforce.ibmcloud.com/vulnerabilities/203906	A-IBM-JAZZ-061021/160
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204279. **CVE ID : CVE-2021-29810**	https://www.ibm.com/support/pages/node/6491547, https://exchange.xforce.ibmcloud.com/vulnerabilities/204279	A-IBM-JAZZ-061021/161
Improper Neutralization of Input During Web Page	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-	https://exchange.xforce.ibmcloud.com/vulnerabilities/204330,	A-IBM-JAZZ-061021/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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: 204330. **CVE ID : CVE-2021-29812**	https://www.ibm.com/support/pages/node/6491545	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204331. **CVE ID : CVE-2021-29813**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204331, https://www.ibm.com/support/pages/node/6491543	A-IBM-JAZZ-061021/163
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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	https://www.ibm.com/support/pages/node/6491539, https://exchange.xforce.ibmcloud.com/vulnerabilities/204334	A-IBM-JAZZ-061021/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session. IBM X-Force ID: 204334. **CVE ID : CVE-2021-29814**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204340. **CVE ID : CVE-2021-29815**	https://www.ibm.com/support/pages/node/6491537, https://exchange.xforce.ibmcloud.com/vulnerabilities/204340	A-IBM-JAZZ-061021/165
Cross-Site Request Forgery (CSRF)	23-Sep-21	4.3	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 204341. **CVE ID : CVE-2021-29816**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204341, https://www.ibm.com/support/pages/node/6491535	A-IBM-JAZZ-061021/166
Improper Restriction of XML External Entity Reference	21-Sep-21	5.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker	https://www.ibm.com/support/pages/node/6490905	A-IBM-JAZZ-061021/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 204775. **CVE ID : CVE-2021-29831**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204824. **CVE ID : CVE-2021-29832**	https://www.ibm.com/support/pages/node/6491529, https://exchange.xforce.ibmcloud.com/vulnerabilities/204824	A-IBM-JAZZ-061021/168
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204825. **CVE ID : CVE-2021-29833**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204825, https://www.ibm.com/support/pages/node/6491527	A-IBM-JAZZ-061021/169
Cleartext	23-Sep-21	2.1	IBM Jazz for Service	https://ww	A-IBM-JAZZ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Storage of Sensitive Information			Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI displays user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 207610. **CVE ID : CVE-2021-29904**	w.ibm.com/support/pages/node/6491525, https://exchange.xforce.ibmcloud.com/vulnerabilities/207610	061021/170
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI 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: 207616. **CVE ID : CVE-2021-29905**	https://www.ibm.com/support/pages/node/6491523, https://exchange.xforce.ibmcloud.com/vulnerabilities/207616	A-IBM-JAZZ-061021/171
security_guardium					
Generation of Error Message Containing Sensitive Information	23-Sep-21	4	IBM Security Guardium 11.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 195569. **CVE ID : CVE-2021-20377**	https://www.ibm.com/support/pages/node/6491125, https://exchange.xforce.ibmcloud.com/vulnerabilities/195569	A-IBM-SECU-061021/172
security_verify_bridge					
Insufficiently Protected	23-Sep-21	2.1	IBM Security Verify Bridge 1.0.5.0 stores user credentials	https://exchange.xforce.i	A-IBM-SECU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			in plain clear text which can be read by a locally authenticated user. IBM X-Force ID: 208154. **CVE ID : CVE-2021-38863**	bmcloud.com/vulnerabilities/208154, https://www.ibm.com/support/pages/node/6491653	061021/173
Improper Certificate Validation	23-Sep-21	5	IBM Security Verify Bridge 1.0.5.0 could allow a user to obtain sensitive information due to improper certificate validation. IBM X-Force ID: 208155. **CVE ID : CVE-2021-38864**	https://exchange.xforce.ibmcloud.com/vulnerabilities/208155, https://www.ibm.com/support/pages/node/6491651	A-IBM-SECU-061021/174
Insufficiently Protected Credentials	23-Sep-21	2.1	IBM Security Verify Bridge 1.0.5.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 196346. **CVE ID : CVE-2021-20434**	https://exchange.xforce.ibmcloud.com/vulnerabilities/196346, https://www.ibm.com/support/pages/node/6491651	A-IBM-SECU-061021/175
Improper Certificate Validation	23-Sep-21	2.1	IBM Security Verify Bridge 1.0.5.0 does not properly validate a certificate which could allow a local attacker to obtain sensitive information that could aid in further attacks against the system. IBM X-Force ID: 196355. **CVE ID : CVE-2021-20435**	https://www.ibm.com/support/pages/node/6491651, https://exchange.xforce.ibmcloud.com/vulnerabilities/196355	A-IBM-SECU-061021/176
sterling_file_gateway					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Sterling File Gateway 2.2.0.0 through 6.1.0.3 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: 197666. **CVE ID : CVE-2021-20484**	https://www.ibm.com/support/pages/node/6491647, https://exchange.xforce.ibmcloud.com/vulnerabilities/197666	A-IBM-STER-061021/177
Generation of Error Message Containing Sensitive Information	23-Sep-21	4	IBM Sterling File Gateway 2.2.0.0 through 6.1.0.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 197667. **CVE ID : CVE-2021-20485**	https://www.ibm.com/support/pages/node/6491645, https://exchange.xforce.ibmcloud.com/vulnerabilities/197667	A-IBM-STER-061021/178
Exposure of Sensitive Information to an Unauthorized Actor	23-Sep-21	4	IBM Sterling File Gateway 2.2.0.0 through 6.1.0.3 could allow a remote authenciated user to obtain sensitive information. By sending a specially crafted request, the user could disclose a valid filepath on the server which could be used in further attacks against the system. IBM X-Force ID: 199234. **CVE ID : CVE-2021-20563**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199234, https://www.ibm.com/support/pages/node/6491645	A-IBM-STER-061021/179
sterling_order_management					
Improper	30-Sep-21	4.3	IBM Sterling Order	https://ww	A-IBM-STER-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Management 9.4, 9.5, and 10.0 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: 199179. **CVE ID : CVE-2021-20554**	w.ibm.com/support/pages/node/6493881	061021/180
tivoli_netcool\\/omnibus_gui					
Improper Restriction of XML External Entity Reference	21-Sep-21	5.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 204775. **CVE ID : CVE-2021-29831**	https://www.ibm.com/support/pages/node/6490905	A-IBM-TIVO-061021/181
tivoli_netcool\\/omnibus_webgui					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Tivoli Netcool/OMNIbus_GUI and IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	https://www.ibm.com/support/pages/node/6491109, https://exchange.xforce.ibmcloud.com/vulnerabilities/203906	A-IBM-TIVO-061021/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functionality potentially leading to credentials disclosure within a trusted session. **CVE ID : CVE-2021-29800**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored 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: 204264. **CVE ID : CVE-2021-29806**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204264, https://www.ibm.com/support/pages/node/6490747	A-IBM-TIVO-061021/183
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored 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: 204265. **CVE ID : CVE-2021-29807**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204265, https://www.ibm.com/support/pages/node/6490747	A-IBM-TIVO-061021/184
Improper Neutralization of Input During Web	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-	https://exchange.xforce.ibmcloud.com/vulnerabiliti	A-IBM-TIVO-061021/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			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: 204269. **CVE ID : CVE-2021-29808**	es/204269, https://www.ibm.com/support/pages/node/6490747	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored 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: 204270. **CVE ID : CVE-2021-29809**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204270, https://www.ibm.com/support/pages/node/6490747	A-IBM-TIVO-061021/186
Insufficiently Protected Credentials	20-Sep-21	4	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 stores user credentials in plain clear text which can be read by an authenticated admin user. IBM X-Force ID: 204329. **CVE ID : CVE-2021-29811**	https://www.ibm.com/support/pages/node/6490747, https://exchange.xforce.ibmcloud.com/vulnerabilities/204329	A-IBM-TIVO-061021/187
Improper Neutralization of Input	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0	https://exchange.xforce.ibmcloud.com	A-IBM-TIVO-061021/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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: 204343. **CVE ID : CVE-2021-29817**	/vulnerabilities/204343, https://www.ibm.com/support/pages/node/6490747	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 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: 204345. **CVE ID : CVE-2021-29818**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204345, https://www.ibm.com/support/pages/node/6490747	A-IBM-TIVO-061021/189
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 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: 204346. **CVE ID : CVE-2021-29819**	https://www.ibm.com/support/pages/node/6490747	A-IBM-TIVO-061021/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 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: 204347. **CVE ID : CVE-2021-29820**	https://www.ibm.com/support/pages/node/6490747	A-IBM-TIVO-061021/191
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 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: 204348. **CVE ID : CVE-2021-29821**	https://www.ibm.com/support/pages/node/6490747, https://exchange.xforce.ibmcloud.com/vulnerabilities/204348	A-IBM-TIVO-061021/192
N/A	20-Sep-21	4	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 could allow an authenticated usre to cause a denial of service through the WebGUI Map Creation page. IBM X-Force ID: 205685. **CVE ID : CVE-2021-29856**	https://exchange.xforce.ibmcloud.com/vulnerabilities/205685, https://www.ibm.com/support/pages/node/6490747	A-IBM-TIVO-061021/193
websphere_application_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	16-Sep-21	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0 and Liberty 17.0.0.3 through 21.0.0.9 could allow a remote user to enumerate usernames due to a difference of responses from valid and invalid login attempts. IBM X-Force ID: 205202. **CVE ID : CVE-2021-29842**	https://www.ibm.com/support/pages/node/6489485, https://exchange.xforce.ibmcloud.com/vulnerabilities/205202	A-IBM-WEBS-061021/194
inflect_project					
inflect					
Incorrect Comparison	27-Sep-21	5	inflect is vulnerable to Inefficient Regular Expression Complexity **CVE ID : CVE-2021-3820**	https://github.com/pksunkara/inflect/commit/a9a0a8e9561c3487854c7cae42565d9652ec858b, https://huntr.dev/bounties/4612b31a-072b-4f61-a916-c7e4cbc2042a	A-INF-INFL-061021/195
itservicejung					
youforms-free-for-copecart					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The youForms for WordPress plugin through 1.0.5 does not sanitise escape the Button Text field of its Templates, allowing high privilege users (editors and admins) to perform Cross-Site Scripting attacks even when the unfiltered_html capability is	N/A	A-ITS-YOUF-061021/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disallowed **CVE ID : CVE-2021-24596**		
jpeg					
libjpeg					
Incorrect Comparison	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. An uncaught floating point exception in the function ACLosslessScan::ParseMCU() located in aclosslessscan.cpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39514**	N/A	A-JPE-LIBJ-061021/197
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function SampleInterleavedLSScan::ParseMCU() located in sampleinterleavedlsscan.cpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39515**	N/A	A-JPE-LIBJ-061021/198
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function HuffmanDecoder::Get() located in huffmandecoder.hpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39516**	N/A	A-JPE-LIBJ-061021/199
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::Reco	https://github.com/thorfdbg/libjpeg/issues/33	A-JPE-LIBJ-061021/200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			nstructUnsampled() located in blockbitmaprequester.cpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39517**		
Out-of-bounds Write	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. LineBuffer::FetchRegion() in linebuffer.cpp has a heap-based buffer overflow. **CVE ID : CVE-2021-39518**	https://github.com/thorfdbg/libjpeg/issues/35	A-JPE-LIBJ-061021/201
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::PullQData() located in blockbitmaprequester.cpp It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39519**	https://github.com/thorfdbg/libjpeg/issues/28	A-JPE-LIBJ-061021/202
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::PushReconstructedData() located in blockbitmaprequester.cpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39520**	https://github.com/thorfdbg/libjpeg/issues/34	A-JPE-LIBJ-061021/203
jscom					
revoworks_browser					
Exposure of Resource to Wrong Sphere	17-Sep-21	6.8	Improper control of program execution vulnerability in RevoWorks Browser 2.1.230 and earlier allows an attacker to execute an arbitrary	https://jscom.jp/news-20210910_2/	A-JSC-REVO-061021/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command or code via unspecified vectors. **CVE ID : CVE-2021-20790**		
Improper Privilege Management	17-Sep-21	6.4	Improper access control vulnerability in RevoWorks Browser 2.1.230 and earlier allows an attacker to bypass access restriction and to exchange unauthorized files between the local environment and the isolated environment or settings of the web browser via unspecified vectors. **CVE ID : CVE-2021-20791**	https://jscom.jp/news-20210910_2/	A-JSC-REVO-061021/205
jsoneditoronline					
jsoneditor					
Incorrect Comparison	27-Sep-21	5	jsoneditor is vulnerable to Inefficient Regular Expression Complexity **CVE ID : CVE-2021-3822**	https://github.com/josdejong/jsoneditor/commit/092e386cf49f2a1450625617da8e0137ed067c3e, https://huntr.dev/bounties/1e3ed803-b7ed-42f1-a4ea-c4c75da9de73	A-JSO-JSON-061021/206
jsoniter					
jsoniter					
Deserialization of Untrusted Data	19-Sep-21	7.5	All versions of package com.jsoniter:jsoniter are vulnerable to Deserialization of Untrusted Data via	N/A	A-JSO-JSON-061021/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious JSON strings. This may lead to a Denial of Service, and in certain cases, code execution. **CVE ID : CVE-2021-23441**		
jsuites					
jsuites					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-21	3.5	jsuites is an open source collection of common required javascript web components. In affected versions users are subject to cross site scripting (XSS) attacks via clipboard content. jsuites is vulnerable to DOM based XSS if the user can be tricked into copying _anything_ from a malicious and pasting it into the html editor. This is because a part of the clipboard content is directly written to `innerHTML` allowing for javascript injection and thus XSS. Users are advised to update to version 4.9.11 to resolve. **CVE ID : CVE-2021-41086**	https://github.com/jsuites/jsuites/commit/fe1d3cc5e339f2f4da8ed1f9f42271fdf9cbd8d2, https://github.com/jsuites/jsuites/security/advisories/GHSA-qh7x-j4v8-qw5w, https://github.com/jsuites/jsuites/commit/d47a6f4e143188dde2742f4cffd313e1068ad3b3	A-JSU-JSUI-061021/208
Juniper					
libslax					
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in libslax through v0.22.1. slaxLexer() in slaxlexer.c has a stack-based buffer overflow. **CVE ID : CVE-2021-39531**	N/A	A-JUN-LIBS-061021/209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libslax through v0.22.1. A NULL pointer dereference exists in the function slaxLexer() located in slaxlexer.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39532**	N/A	A-JUN-LIBS-061021/210
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in libslax through v0.22.1. slaxLexer() in slaxlexer.c has a heap-based buffer overflow. **CVE ID : CVE-2021-39533**	N/A	A-JUN-LIBS-061021/211
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in libslax through v0.22.1. slaxIsCommentStart() in slaxlexer.c has a heap-based buffer overflow. **CVE ID : CVE-2021-39534**	N/A	A-JUN-LIBS-061021/212
kindsoft					
kindeditor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-21	4.3	Cross Site Scripting (XSS) vulnerability exists in all versions of KindEditor, which can be exploited by an attacker to obtain user cookie information. **CVE ID : CVE-2021-37267**	N/A	A-KIN-KIND-061021/213
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-21	4.3	Cross Site Scripting (XSS) vulnerability exists in KindEditor (Chinese versions) 4.1.12, which can be exploited by an attacker to obtain user cookie information. **CVE ID : CVE-2021-30086**	N/A	A-KIN-KIND-061021/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Kubernetes					
kubernetes					
Externally Controlled Reference to a Resource in Another Sphere	20-Sep-21	3.5	A security issue was discovered with Kubernetes that could enable users to send network traffic to locations they would otherwise not have access to via a confused deputy attack. **CVE ID : CVE-2021-25740**	https://github.com/kubernetes/kubernetes/issues/103675	A-KUB-KUBE-061021/215
Files or Directories Accessible to External Parties	20-Sep-21	5.5	A security issue was discovered in Kubernetes where a user may be able to create a container with subpath volume mounts to access files & directories outside of the volume, including on the host filesystem. **CVE ID : CVE-2021-25741**	https://github.com/kubernetes/kubernetes/issues/104980	A-KUB-KUBE-061021/216
libiff_project					
libiff					
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in libiff through 20190123. A global-buffer-overflow exists in the function IFF_errorId located in error.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-32298**	N/A	A-LIB-LIBI-061021/217
libxsmm_project					
libxsmm					
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libxsmm through v1.16.1-93. A NULL pointer dereference exists in JIT code. It allows an attacker to cause Denial of	N/A	A-LIB-LIBX-061021/218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service. **CVE ID : CVE-2021-39535**		
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in libxsmm through v1.16.1-93. The JIT code has a heap-based buffer overflow. **CVE ID : CVE-2021-39536**	N/A	A-LIB-LIBX-061021/219
lief-project					
lief					
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in LIEF through 0.11.4. A heap-buffer-overflow exists in the function main located in pe_reader.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-32297**	https://github.com/lief-project/LIEF/issues/449	A-LIE-LIEF-061021/220
limit_login_attempts_project					
limit_login_attempts					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	4.3	The Limit Login Attempts WordPress plugin before 4.0.50 does not escape the IP addresses (which can be controlled by attacker via headers such as X-Forwarded-For) of attempted logins before outputting them in the reports table, leading to an Unauthenticated Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24657**	N/A	A-LIM-LIMI-061021/221
Linuxfoundation					
tremor					
Use After Free	17-Sep-21	7.5	Tremor is an event processing system for unstructured data. A	https://github.com/tremor-rs/tremor-	A-LIN-TREM-061021/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists between versions 0.7.2 and 0.11.6. This vulnerability is a memory safety Issue when using `patch` or `merge` on `state` and assign the result back to `state`. In this case, affected versions of Tremor and the tremor-script crate maintains references to memory that might have been freed already. And these memory regions can be accessed by retrieving the `state`, e.g. send it over TCP or HTTP. This requires the Tremor server (or any other program using tremor-script) to execute a tremor-script script that uses the mentioned language construct. The issue has been patched in version 0.11.6 by removing the optimization and always cloning the target expression of a Merge or Patch. If an upgrade is not possible, a possible workaround is to avoid the optimization by introducing a temporary variable and not immediately reassigning to `state`. **CVE ID : CVE-2021-39228**	runtime/pull/1217, https://github.com/tremor-rs/tremor-runtime/commit/1a2efcdbe68e5e7fd0a05836ac32d2cde78a0b2e, https://github.com/tremor-rs/tremor-runtime/security/advisories/GHSA-mc22-5q92-8v85	
linuxsampler					
libgig					
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in libgig through 20200507. A heap-buffer-overflow exists in the function	N/A	A-LIN-LIBG-061021/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RIFF::List::GetSubList located in RIFF.cpp. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-32294**		
lodash					
lodash					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Sep-21	7.5	** DISPUTED ** A command injection vulnerability in Lodash 4.17.21 allows attackers to achieve arbitrary code execution via the template function. This is a different parameter, method, and version than CVE-2021-23337. NOTE: the vendor's position is that it's the developer's responsibility to ensure that a template does not evaluate code that originates from untrusted input. **CVE ID : CVE-2021-41720**	N/A	A-LOD-LODA-061021/224
maianaffiliate					
maianaffiliate					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-21	3.5	MaianAffiliate v1.0 allows an authenticated administrative user to save an XSS to the database. **CVE ID : CVE-2021-39404**	N/A	A-MAI-MAIA-061021/225
Maianscriptworld					
maianaffiliate					
Improper Neutralizatio	20-Sep-21	3.5	MaianAffiliate v.1.0 is suffers from code injection by adding	https://www.maianscrip	A-MAI-MAIA-061021/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			a new product via the admin panel. The injected payload is reflected on the affiliate main page for all authenticated and unauthenticated visitors. **CVE ID : CVE-2021-39402**	tworld.co.uk/	
Manageengine					
desktop_central					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	21-Sep-21	7.5	ManageEngine Desktop Central before build 10.0.683 allows Unauthenticated Remote Code Execution during communication with Notification Server. **CVE ID : CVE-2021-28960**	https://www.manageengine.com/products/desktop-central/unauthenticated-command-injection-vulnerability.html	A-MAN-DESK-061021/227
Mcafee					
data_loss_prevention_discover					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Sep-21	6	A buffer overflow vulnerability in McAfee Data Loss Prevention (DLP) Discover prior to 11.6.100 allows an attacker in the same network as the DLP Discover to execute arbitrary code through placing carefully constructed Ami Pro (.sam) files onto a machine and having DLP Discover scan it, leading to remote code execution with elevated privileges. This is caused by the destination buffer being of fixed size and incorrect checks being made on the	https://kc.mcafee.com/corporate/index?page=content&id=SB10368	A-MCA-DATA-061021/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			source size. **CVE ID : CVE-2021-31845**		
data_loss_prevention_endpoint					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Sep-21	4.6	A buffer overflow vulnerability in McAfee Data Loss Prevention (DLP) Endpoint for Windows prior to 11.6.200 allows a local attacker to execute arbitrary code with elevated privileges through placing carefully constructed Ami Pro (.sam) files onto the local system and triggering a DLP Endpoint scan through accessing a file. This is caused by the destination buffer being of fixed size and incorrect checks being made on the source size. **CVE ID : CVE-2021-31844**	https://kc.mcafee.com/corporate/index?page=content&id=SB10368	A-MCA-DATA-061021/229
endpoint_security					
Improper Restriction of XML External Entity Reference	17-Sep-21	2.1	XML Entity Expansion injection vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2021 Update allows a local user to initiate high CPU and memory consumption resulting in a Denial of Service attack through carefully editing the EPDeploy.xml file and then executing the setup process. **CVE ID : CVE-2021-31842**	https://kc.mcafee.com/corporate/index?page=content&id=SB10367	A-MCA-ENDP-061021/230
Improper Privilege Management	17-Sep-21	4.6	Improper privileges management vulnerability in McAfee Endpoint Security	https://kc.mcafee.com/corporate/inde	A-MCA-ENDP-061021/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(ENS) Windows prior to 10.7.0 September 2021 Update allows local users to access files which they would otherwise not have access to via manipulating junction links to redirect McAfee folder operations to an unintended location. **CVE ID : CVE-2021-31843**	x?page=content&id=SB10367	
mcafee_agent					
Improper Privilege Management	22-Sep-21	3.6	Improper privilege management vulnerability in maconfig for McAfee Agent for Windows prior to 5.7.4 allows a local user to gain access to sensitive information. The utility was able to be run from any location on the file system and by a low privileged user. **CVE ID : CVE-2021-31836**	https://kc.mcafee.com/corporate/index?page=content&id=SB10369	A-MCA-MCAF-061021/232
Untrusted Search Path	22-Sep-21	6.9	A DLL sideloading vulnerability in McAfee Agent for Windows prior to 5.7.4 could allow a local user to perform a DLL sideloading attack with an unsigned DLL with a specific name and in a specific location. This would result in the user gaining elevated permissions and the ability to execute arbitrary code as the system user, through not checking the DLL signature. **CVE ID : CVE-2021-31841**	https://kc.mcafee.com/corporate/index?page=content&id=SB10369	A-MCA-MCAF-061021/233
Improper Verification	22-Sep-21	6.9	Improper access control vulnerability in the repair	https://kc.mcafee.com/co	A-MCA-MCAF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Cryptographic Signature			process for McAfee Agent for Windows prior to 5.7.4 could allow a local attacker to perform a DLL preloading attack using unsigned DLLs. This would result in elevation of privileges and the ability to execute arbitrary code as the system user, through not correctly protecting a temporary directory used in the repair process and not checking the DLL signature. **CVE ID : CVE-2021-31847**	rporate/index?page=content&id=SB10369	061021/234
Microfocus					
arcsight_enterprise_security_manager					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	28-Sep-21	7.5	Remote Code Execution vulnerability in Micro Focus ArcSight Enterprise Security Manager (ESM) product, affecting versions 7.0.2 through 7.5. The vulnerability could be exploited resulting in remote code execution. **CVE ID : CVE-2021-38124**	https://portal.microfocus.com/s/article/KM000001960	A-MIC-ARCS-061021/235
Misp					
misp					
N/A	17-Sep-21	7.5	In MISP before 2.4.148, app/Lib/Export/OpendataExport.php mishandles parameter data that is used in a shell_exec call. **CVE ID : CVE-2021-41326**	https://github.com/MISP/MISP/commit/e36f739470f0c42199acd1a94c7051e741bc97320	A-MIS-MISP-061021/236
mitmproxy					
mitmproxy					
Inconsistent	16-Sep-21	7.5	mitmproxy is an interactive,	https://githu	A-MIT-MITM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Interpretation of HTTP Requests ('HTTP Request Smuggling')			SSL/TLS-capable intercepting proxy. In mitmproxy 7.0.2 and below, a malicious client or server is able to perform HTTP request smuggling attacks through mitmproxy. This means that a malicious client/server could smuggle a request/response through mitmproxy as part of another request/response's HTTP message body. While a smuggled request is still captured as part of another request's body, it does not appear in the request list and does not go through the usual mitmproxy event hooks, where users may have implemented custom access control checks or input sanitization. Unless one uses mitmproxy to protect an HTTP/1 service, no action is required. The vulnerability has been fixed in mitmproxy 7.0.3 and above. **CVE ID : CVE-2021-39214**	b.com/mitmproxy/mitmproxy/security/advisories/GHSA-22gh-3r9q-xf38	061021/237
motopress					
timetable_and_event_schedule					
Improper Access Control	20-Sep-21	4.3	The Timetable and Event Schedule WordPress plugin before 2.4.2 does not have proper access control when deleting a timeslot, allowing any user with the edit_posts capability (contributor+) to delete arbitrary timeslot from any events. Furthermore, no CSRF check is in place as well,	N/A	A-MOT-TIME-061021/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowing such attack to be performed via CSRF against a logged in with such capability **CVE ID : CVE-2021-24583**		
Improper Access Control	20-Sep-21	3.5	The Timetable and Event Schedule WordPress plugin before 2.4.2 does not have proper access control when updating a timeslot, allowing any user with the edit_posts capability (contributor+) to update arbitrary timeslot from any events. Furthermore, no CSRF check is in place as well, allowing such attack to be perform via CSRF against a logged in with such capability. In versions before 2.3.19, the lack of sanitisation and escaping in some of the fields, like the descritption could also lead to Stored XSS issues **CVE ID : CVE-2021-24584**	N/A	A-MOT-TIME-061021/239
Exposure of Sensitive Information to an Unauthorized Actor	20-Sep-21	4	The Timetable and Event Schedule WordPress plugin before 2.4.0 outputs the Hashed Password, Username and Email Address (along other less sensitive data) of the user related to the Even Head of the Timeslot in the response when requesting the event Timeslot data with a user with the edit_posts capability. Combined with the other Unauthorised Event Timeslot Modification issue (https://wpscan.com/reports/submissions/4699/) where	N/A	A-MOT-TIME-061021/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an arbitrary user ID can be set, this could allow low privilege users with the edit_posts capability (such as author) to retrieve sensitive User data by iterating over the user_id **CVE ID : CVE-2021-24585**		
Nagios					
nagios_xi					
Incorrect Default Permissions	28-Sep-21	7.5	Nagios XI before 5.8.5 has Incorrect Permission Assignment for migrate.php. **CVE ID : CVE-2021-36363**	https://www.nagios.com/downloads/nagios-xi/change-log/, https://assets.nagios.com/downloads/nagiosxi/CHANGES-5.TXT	A-NAG-NAGI-061021/241
Incorrect Default Permissions	28-Sep-21	7.5	Nagios XI before 5.8.5 has Incorrect Permission Assignment for repairmysql.sh. **CVE ID : CVE-2021-36365**	https://www.nagios.com/downloads/nagios-xi/change-log/, https://assets.nagios.com/downloads/nagiosxi/CHANGES-5.TXT	A-NAG-NAGI-061021/242
netmotionsoftware					
mobility					
Incorrect Permission	16-Sep-21	4	The access controls on the Mobility read-only API	https://www.netmotion	A-NET-MOBI-061021/243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assignment for Critical Resource			improperly validate user access permissions. Attackers with both network access to the API and valid credentials can read data from it; regardless of access control group membership settings. This vulnerability is fixed in Mobility v11.76 and Mobility v12.14. **CVE ID : CVE-2021-40066**	software.com/security-advisories/cve-2021-40066	
Incorrect Permission Assignment for Critical Resource	16-Sep-21	4.9	The access controls on the Mobility read-write API improperly validate user access permissions; this API is disabled by default. If the API is manually enabled, attackers with both network access to the API and valid credentials can read and write data to it; regardless of access control group membership settings. This vulnerability is fixed in Mobility v12.14. **CVE ID : CVE-2021-40067**	https://www.netmotionsoftware.com/security-advisories/cve-2021-40067	A-NET-MOBI-061021/244
NI					
ni-pal					
Improper Input Validation	17-Sep-21	4.6	Improper input validation in the National Instruments NI-PAL driver in versions 20.0.0 and prior may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-38304**	https://www.ni.com/en-us/support/documentation/supplemental/21/improper-input-validation-in-ni-pal.html	A-NI-NI-P-061021/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Ninjaforms					
ninja_forms					
Incorrect Authorization	22-Sep-21	4	The Ninja Forms WordPress plugin is vulnerable to sensitive information disclosure via the bulk_export_submissions function found in the ~/includes/Routes/Submissions.php file, in versions up to and including 3.5.7. This allows authenticated attackers to export all Ninja Forms submissions data via the /ninja-forms-submissions/export REST API which can include personally identifiable information. **CVE ID : CVE-2021-34647**	https://plugins.trac.wordpress.org/browser/ninja-forms/trunk/includes/Routes/Submissions.php?rev=2543837#L107	A-NIN-NINJ-061021/246
Incorrect Authorization	22-Sep-21	4	The Ninja Forms WordPress plugin is vulnerable to arbitrary email sending via the trigger_email_action function found in the ~/includes/Routes/Submissions.php file, in versions up to and including 3.5.7. This allows authenticated attackers to send arbitrary emails from the affected server via the /ninja-forms-submissions/email-action REST API which can be used to socially engineer victims. **CVE ID : CVE-2021-34648**	https://plugins.trac.wordpress.org/browser/ninja-forms/trunk/includes/Routes/Submissions.php?rev=2543837#L155	A-NIN-NINJ-061021/247
nltk					
nltk					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Comparison	27-Sep-21	5	nltk is vulnerable to Inefficient Regular Expression Complexity **CVE ID : CVE-2021-3828**	https://huntr.dev/bounties/d19aed43-75bc-4a03-91a0-4d0bb516bc32, https://github.com/nltk/nltk/commit/277711ab1dec729e626b27aab6fa35ea5efbd7e6	A-NLT-NLTK-061021/248
Nokia					
heif					
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in heif through v3.6.2. A global-buffer-overflow exists in the function HevcDecoderConfigurationRecord::getPicWidth() located in hevcdecoderconfigrecord.cpp. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-32287**	N/A	A-NOK-HEIF-061021/249
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in heif through v3.6.2. A global-buffer-overflow exists in the function HevcDecoderConfigurationRecord::getPicHeight() located in hevcdecoderconfigrecord.cpp. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-32288**	https://github.com/nokiatech/heif/issues/87	A-NOK-HEIF-061021/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in heif through through v3.6.2. A NULL pointer dereference exists in the function convertByteStreamToRBSP() located in nalutil.cpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-32289**	https://github.com/nokiatech/heif/issues/85	A-NOK-HEIF-061021/251
nth-check_project					
nth-check					
N/A	17-Sep-21	5	nth-check is vulnerable to Inefficient Regular Expression Complexity **CVE ID : CVE-2021-3803**	https://github.com/fb55/nth-check/commit/9894c1d2010870c351f66c6f6efcf656e26bb726, https://huntr.dev/bounties/8cf8cc06-d2cf-4b4e-b42c-99fafb0b04d0	A-NTH-NTH--061021/252
object-path_project					
object-path					
Improperly Controlled Modification of Dynamically-Determined Object Attributes	17-Sep-21	5	object-path is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') **CVE ID : CVE-2021-3805**	https://huntr.dev/bounties/571e3baf-7c46-46e3-9003-ba7e4e623053, https://github.com/mariocasciaro/object-	A-OBJ-OBJE-061021/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				path/commit/e6bb638ffdd431176701b3e9024f80050d0ef0a6	
octopus					
halibut					
Deserialization of Untrusted Data	22-Sep-21	10	In Halibut versions prior to 4.4.7 there is a deserialisation vulnerability that could allow remote code execution on systems that already trust each other based on certificate verification. **CVE ID : CVE-2021-31819**	https://advisories.octopus.com/adv/2021-08---Remote-Code-Execution-via-Deserialisation-in-the-Halibut-Protocol-(CVE-2021-31819).2250309681.html	A-OCT-HALI-061021/254
offshorewebmaster					
availability_calendar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The Availability Calendar WordPress plugin before 1.2.2 does not sanitise or escape its Category Names before outputting them in page/post where the associated shortcode is embed, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed **CVE ID : CVE-2021-24604**	N/A	A-OFF-AVAI-061021/255
Improper	20-Sep-21	6.5	The Availability Calendar	N/A	A-OFF-AVAI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			WordPress plugin before 1.2.1 does not escape the category attribute from its shortcode before using it in a SQL statement, leading to a SQL Injection issue, which can be exploited by any user able to add shortcode to posts/pages, such as contributor+ **CVE ID : CVE-2021-24606**		061021/256
ombu					
the_sorter					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The check_order function of The Sorter WordPress plugin through 1.0 uses an `area_id` parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. **CVE ID : CVE-2021-24399**	N/A	A-OMB-THE_-061021/257
Openbsd					
libressl					
Out-of-bounds Read	24-Sep-21	4.3	x509_constraints_parse_mailbox in lib/libcrypto/x509/x509_constraints.c in LibreSSL through 3.4.0 has a stack-based buffer over-read. When the input exceeds DOMAIN_PART_MAX_LEN, the buffer lacks '\0' termination. **CVE ID : CVE-2021-41581**	https://github.com/libressl-portable/openbsd/issues/126	A-OPE-LIBR-061021/258
openssh					
Improper	26-Sep-21	6	sshd in OpenSSH 6.2 through	https://ww	A-OPE-OPEN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user. **CVE ID : CVE-2021-41617**	w.openssh.com/txt/release-8.8, https://www.openssh.com/security.html, https://bugzilla.suse.com/show_bug.cgi?id=1190975	061021/259
Openvpn					
openvpn_access_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	4.3	OpenVPN Access Server 2.9.0 through 2.9.4 allow remote attackers to inject arbitrary web script or HTML via the web login page URL. **CVE ID : CVE-2021-3824**	https://openvpn.net/vpn-server-resources/release-notes/#openvpn-access-server-2-9-5	A-OPE-OPEN-061021/260
openvpn-monitor_project					
openvpn-monitor					
Cross-Site Request Forgery (CSRF)	27-Sep-21	4.3	furlongm openvpn-monitor through 1.1.3 allows CSRF to disconnect an arbitrary client. **CVE ID : CVE-2021-31604**	N/A	A-OPE-OPEN-061021/261
Improper Neutralization of Special Elements used in a	27-Sep-21	7.8	furlongm openvpn-monitor through 1.1.3 allows %0a command injection via the OpenVPN management interface socket. This can	N/A	A-OPE-OPEN-061021/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			shut down the server via signal%20SIGTERM. **CVE ID : CVE-2021-31605**		
Improper Authenticati on	27-Sep-21	5	furlongm openvpn-monitor through 1.1.3 allows Authorization Bypass to disconnect arbitrary clients. **CVE ID : CVE-2021-31606**	N/A	A-OPE-OPEN-061021/263
optinmonster					
optinmonster					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	4.3	The OptinMonster WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient input validation in the load_previews function found in the ~/OMAPI/Output.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.6.0. **CVE ID : CVE-2021-39325**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2595758%40optinmonster&new=2595758%40optinmonster&sfp_email=&sfph_mail=#file2	A-OPT-OPTI-061021/264
os4ed					
opensis					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	24-Sep-21	6.5	A SQL injection vulnerability exists in the Take Attendance functionality of OS4Ed's OpenSIS 8.0. allows an attacker to inject their own SQL query. The cp_id_miss_attn parameter from TakeAttendance.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request	N/A	A-OS4-OPEN-061021/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as a user with access to "Take Attendance" functionality to trigger this vulnerability. **CVE ID : CVE-2021-40309**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Sep-21	3.5	OpenSIS Community Edition version 8.0 is affected by a cross-site scripting (XSS) vulnerability in the TakeAttendance.php via the cp_id_miss_attn parameter. **CVE ID : CVE-2021-40310**	N/A	A-OS4-OPEN-061021/266
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-21	4.3	OpenSIS Community Edition version <= 7.6 is affected by a reflected XSS vulnerability in EmailCheck.php via the "opt" parameter. **CVE ID : CVE-2021-27340**	https://github.com/OS4ED/openSIS-Classic/commit/f78407d5291c686c3f416073dcb9143f3a3d5489#diff-24b751f2072f058259d03301693810 1f9fa29884ebcc09ce7eb88def3421e5ba	A-OS4-OPEN-061021/267
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Sep-21	7.5	OpenSIS Community Edition version <= 7.6 is affected by a local file inclusion vulnerability in DownloadWindow.php via the "filename" parameter. **CVE ID : CVE-2021-27341**	https://github.com/OS4ED/openSIS-Classic/commit/f78407d5291c686c3f416073dcb9143f3a3d5489#diff-24b751f2072f058259d03301693810	A-OS4-OPEN-061021/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1f9fa29884ebcc09ce7eb88def3421e5ba	
Pandasecurity					
panda_adaptive_defense_360					
Uncontrolled Search Path Element	23-Sep-21	4.4	DLL hijacking in Panda Agent <=1.16.11 in Panda Security, S.L.U. Panda Adaptive Defense 360 <= 8.0.17 allows attacker to escalate privileges via maliciously crafted DLL file. **CVE ID : CVE-2021-26750**	N/A	A-PAN-PAND-061021/269
panda_devices_agent					
Uncontrolled Search Path Element	23-Sep-21	4.4	DLL hijacking in Panda Agent <=1.16.11 in Panda Security, S.L.U. Panda Adaptive Defense 360 <= 8.0.17 allows attacker to escalate privileges via maliciously crafted DLL file. **CVE ID : CVE-2021-26750**	N/A	A-PAN-PAND-061021/270
payara					
micro_community					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Sep-21	5	Payara Micro Community 5.2021.6 and below allows Directory Traversal. **CVE ID : CVE-2021-41381**	https://www.payara.fish	A-PAY-MICR-061021/271
pbrt_project					
pbrt					
Out-of-bounds	20-Sep-21	6.8	An issue was discovered in pbrt through 20200627. A	N/A	A-PBR-PBRT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			stack-buffer-overflow exists in the function pbrt::ParamSet::ParamSet() located in paramset.h. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-32299**		061021/272
pdftools_project					
pdftools					
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function node::ObjNode::Value() located in objnode.cpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39538**	N/A	A-PDF-PDFT-061021/273
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function node::BDCNode::~BDCNode() located in bdcnode.cpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39539**	N/A	A-PDF-PDFT-061021/274
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in pdftools through 20200714. A stack-buffer-overflow exists in the function Analyze::AnalyzePages() located in analyze.cpp. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-39540**	N/A	A-PDF-PDFT-061021/275
NULL Pointer	20-Sep-21	4.3	An issue was discovered in pdftools through 20200714.	N/A	A-PDF-PDFT-061021/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			A NULL pointer dereference exists in the function Analyze::AnalyzeXref() located in analyze.cpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39541**		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function Font::Size() located in font.cpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39542**	N/A	A-PDF-PDFT-061021/277
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function Analyze::AnalyzeRoot() located in analyze.cpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39543**	N/A	A-PDF-PDFT-061021/278
pi-hole					
web_interface					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-21	4.3	adminlte is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3811**	https://huntr.dev/bounties/fa38c61f-4043-4872-bc85-7fe5ae5cc2e8, https://github.com/pi-hole/adminlte/commit/f526716de7bb	A-PI--WEB_-061021/279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				0fd382a64bcbbb33915c926f94bb	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-21	4.3	adminlte is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2021-3812**	https://huntr.dev/bounties/875a6885-9a64-46f3-94ad-92f40f989200, https://github.com/pi-hole/adminlte/commit/f526716de7bb0fd382a64bcbbb33915c926f94bb	A-PI--WEB_-061021/280
Pingidentity					
pingaccess					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	24-Sep-21	5	Ping Identity PingAccess before 5.3.3 allows HTTP request smuggling via header manipulation. **CVE ID : CVE-2021-31923**	https://docs.pingidentity.com/bundle/pingaccess-53/page/wco1629833104567.html	A-PIN-PING-061021/281
plasticscm					
plastic_scm					
N/A	22-Sep-21	5	Plastic SCM before 10.0.16.5622 mishandles the WebAdmin server management interface. **CVE ID : CVE-2021-41382**	https://www.plasticscm.com/download/releasenotes/10.0.16.5622	A-PLA-PLAS-061021/282
print_my_blog_project					
print_my_blog					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	20-Sep-21	5.8	The Print My Blog WordPress Plugin before 3.4.2 does not enforce nonce (CSRF) checks, which allows attackers to make logged in administrators deactivate the Print My Blog plugin and delete all saved data for that plugin by tricking them to open a malicious link **CVE ID : CVE-2021-24636**	N/A	A-PRI-PRIN-061021/283
Realvnc					
vnc_viewer					
Improper Input Validation	17-Sep-21	4.3	** DISPUTED ** RealVNC Viewer 6.21.406 allows remote VNC servers to cause a denial of service (application crash) via crafted RFB protocol data. NOTE: It is asserted that this issue requires social engineering a user into connecting to a fake VNC Server. The VNC Viewer application they are using will then hang, until terminated, but no memory leak occurs - the resources are freed once the hung process is terminated and the resource usage is constant during the hang. Only the process that is connected to the fake Server is affected. This is an application bug, not a security issue. **CVE ID : CVE-2021-41380**	N/A	A-REA-VNC_-061021/284
Revive-adserver					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
revive_adserver					
Use of a Broken or Risky Cryptographic Algorithm	23-Sep-21	4.3	Vulnerability in the generation of session IDs in revive-adserver < 5.3.0, based on the cryptographically insecure uniqid() PHP function. Under some circumstances, an attacker could theoretically be able to brute force session IDs in order to take over a specific account. **CVE ID : CVE-2021-22948**	https://www.revive-adserver.com/security/revive-sa-2021-005/	A-REV-REVI-061021/285
schiocco					
support_board_-_chat_and_help_desk					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	7.5	The Support Board WordPress plugin before 3.3.4 does not escape multiple POST parameters (such as status_code, department, user_id, conversation_id, conversation_status_code, and recipient_id) before using them in SQL statements, leading to SQL injections which are exploitable by unauthenticated users. **CVE ID : CVE-2021-24741**	https://board.support/changes	A-SCH-SUPP-061021/286
seatd_project					
seatd					
Improper Privilege Management	17-Sep-21	8.5	seatd-launch in seatd 0.6.x before 0.6.2 allows privilege escalation because it uses execlp and may be installed setuid root. **CVE ID : CVE-2021-41387**	N/A	A-SEA-SEAT-061021/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sela_project					
sela					
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in sela through 20200412. file::WavFile::writeToFile() in wav_file.c has a heap-based buffer overflow. **CVE ID : CVE-2021-39544**	N/A	A-SEL-SELA-061021/288
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function rice::RiceDecoder::process() located in rice_decoder.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39545**	N/A	A-SEL-SELA-061021/289
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in sela through 20200412. rice::RiceDecoder::process() in rice_decoder.cpp has a heap-based buffer overflow. **CVE ID : CVE-2021-39546**	N/A	A-SEL-SELA-061021/290
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function lpc::SampleGenerator::process() located in sample_generator.cpp. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39547**	N/A	A-SEL-SELA-061021/291
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function frame::FrameDecoder::proces	N/A	A-SEL-SELA-061021/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			s() located in frame_decoder.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39548**		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function file::WavFile::WavFile() located in wav_file.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39549**	N/A	A-SEL-SELA-061021/293
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in sela through 20200412. file::SelaFile::readFromFile() in sela_file.cpp has a heap-based buffer overflow. **CVE ID : CVE-2021-39550**	N/A	A-SEL-SELA-061021/294
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in sela through 20200412. file::SelaFile::readFromFile() in sela_file.c has a heap-based buffer overflow. **CVE ID : CVE-2021-39551**	N/A	A-SEL-SELA-061021/295
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in sela through 20200412. file::WavFile::readFromFile() in wav_file.c has a heap-based buffer overflow. **CVE ID : CVE-2021-39552**	N/A	A-SEL-SELA-061021/296
set_user_project					
set_user					
N/A	27-Sep-21	7.5	The set_user extension module before 3.0.0 for PostgreSQL allows	https://github.com/pgaudit/set_user/r	A-SET-SET_-061021/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ProcessUtility_hook bypass via set_config. **CVE ID : CVE-2021-41558**	eleases/tag/REL3_0_0	
sharpcompress_project					
sharpcompress					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Sep-21	4	SharpCompress is a fully managed C# library to deal with many compression types and formats. Versions prior to 0.29.0 are vulnerable to partial path traversal. SharpCompress recreates a hierarchy of directories under destinationDirectory if ExtractFullPath is set to true in options. In order to prevent extraction outside the destination directory the destinationFileName path is verified to begin with fullDestinationDirectoryPath. However, prior to version 0.29.0, it is not enforced that fullDestinationDirectoryPath ends with slash. If the destinationDirectory is not slash terminated like `/home/user/dir` it is possible to create a file with a name thats begins as the destination directory one level up from the directory, i.e. `/home/user/dir.sh`. Because of the file name and destination directory constraints the arbitrary file creation impact is limited and depends on the use case. This issue is fixed in SharpCompress version	https://github.com/adamhathcock/sharpcompress/security/advisories/GHSA-jp7f-grcv-6mjf, https://github.com/adamhathcock/sharpcompress/pull/614	A-SHA-SHAR-061021/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0.29.0. **CVE ID : CVE-2021-39208**		
Siemens					
solid_edge					
Out-of-bounds Read	28-Sep-21	4.3	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13565). **CVE ID : CVE-2021-41533**	https://cert-portal.siemens.com/productcert/pdf/ssa-728618.pdf	A-SIE-SOLI-061021/299
Out-of-bounds Read	28-Sep-21	4.3	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13703). **CVE ID : CVE-2021-41534**	https://cert-portal.siemens.com/productcert/pdf/ssa-728618.pdf	A-SIE-SOLI-061021/300
Use After Free	28-Sep-21	6.8	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while	https://cert-portal.siemens.com/productcert/pdf/ssa-728618.pdf	A-SIE-SOLI-061021/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13771). **CVE ID : CVE-2021-41535**		
Use After Free	28-Sep-21	6.8	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13778). **CVE ID : CVE-2021-41536**	https://cert-portal.siemens.com/productcert/pdf/ssa-728618.pdf	A-SIE-SOLI-061021/302
Use After Free	28-Sep-21	6.8	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13789). **CVE ID : CVE-2021-41537**	https://cert-portal.siemens.com/productcert/pdf/ssa-728618.pdf	A-SIE-SOLI-061021/303
Access of Uninitialized Pointer	28-Sep-21	4.3	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to information disclosure by unexpected access to an uninitialized pointer while parsing user-supplied OBJ	https://cert-portal.siemens.com/productcert/pdf/ssa-728618.pdf	A-SIE-SOLI-061021/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			files. An attacker could leverage this vulnerability to leak information from unexpected memory locations (ZDI-CAN-13770). **CVE ID : CVE-2021-41538**		
Use After Free	28-Sep-21	6.8	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13773). **CVE ID : CVE-2021-41539**	https://cert-portal.siemens.com/productcert/pdf/ssa-728618.pdf	A-SIE-SOLI-061021/305
Use After Free	28-Sep-21	6.8	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a use-after-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13776). **CVE ID : CVE-2021-41540**	https://cert-portal.siemens.com/productcert/pdf/ssa-728618.pdf	A-SIE-SOLI-061021/306
simple_schools_staff_directory_project					
simple_schools_staff_directory					
Unrestricted Upload of File with Dangerous Type	20-Sep-21	6.5	The Simple Schools Staff Directory WordPress plugin through 1.1 does not validate uploaded logo pictures to ensure that are indeed images, allowing high	N/A	A-SIM-SIMP-061021/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege users such as admin to upload arbitrary file like PHP, leading to RCE **CVE ID : CVE-2021-24663**		
skale					
sgxwallet					
Out-of-bounds Write	27-Sep-21	5	An issue was discovered in SKALE sgxwallet 1.58.3. sgx_disp_ippsAES_GCMEncrypt allows an out-of-bounds write, resulting in a segfault and compromised enclave. This issue describes a buffer overflow, which was resolved prior to v1.77.0 and not reproducible in latest sgxwallet v1.77.0 **CVE ID : CVE-2021-36218**	https://github.com/skalenetwork/sgxwallet/commit/77425c862ad20cd270d42c54f3d63e1eb4e02195	A-SKA-SGXW-061021/308
Access of Uninitialized Pointer	27-Sep-21	7.5	An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address is then freed, resulting in compromised integrity of the enclave. This was resolved after v1.58.3 and not reproducible in sgxwallet v1.77.0. **CVE ID : CVE-2021-36219**	https://github.com/skalenetwork/sgxwallet/commit/4e9b5b7526db083177e81f8bafeaa4914d276a82	A-SKA-SGXW-061021/309
solvercircle					
wp_icommerce					
Improper	20-Sep-21	6.5	The Orders functionality in	N/A	A-SOL-WP_I-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			the WP iCommerce WordPress plugin through 1.1.1 has an `order_id` parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. The feature is available to low privilege users such as contributors **CVE ID : CVE-2021-24402**		061021/310
speed_test_project					
speed_test					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Sep-21	5	e7d Speed Test (aka speedtest) 0.5.3 allows a path-traversal attack that results in information disclosure via the "GET /.." substring. **CVE ID : CVE-2021-40349**	https://old.reddit.com/r/HackingTechniques/comments/poc55t/directory_traversal_bypass_on_e7d_speedtest/	A-SPE-SPEE-061021/311
sqlparse_project					
sqlparse					
Uncontrolled Resource Consumption	20-Sep-21	5	sqlparse is a non-validating SQL parser module for Python. In sqlparse versions 0.4.0 and 0.4.1 there is a regular Expression Denial of Service in sqlparse vulnerability. The regular expression may cause exponential backtracking on strings containing many repetitions of '\r\n' in SQL comments. Only the formatting feature that removes comments from SQL statements is affected by this	https://github.com/andialbrecht/sqlparse/commit/8238a9e450ed1524e40cb3a8b0b3c00606903aeb, https://github.com/andialbrecht/sqlparse/security/advisories/GHSA-p5w8-	A-SQL-SQLP-061021/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			regular expression. As a workaround don't use the sqlformat.format function with keyword strip_comments=True or the --strip-comments command line flag when using the sqlformat command line tool. The issues has been fixed in sqlparse 0.4.2. **CVE ID : CVE-2021-32839**	wqhj-9hhf	
status301					
coolclock					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	3.5	The CoolClock WordPress plugin before 4.3.5 does not escape some shortcode attributes, allowing users with a role as low as Contributor toperform Stored Cross-Site Scripting attacks **CVE ID : CVE-2021-24670**	N/A	A-STA-COOL-061021/313
streama_project					
streama					
Cross-Site Request Forgery (CSRF)	29-Sep-21	6.8	A cross-site request forgery (CSRF) vulnerability exists in Streama up to and including v1.10.3. The application does not have CSRF checks in place when performing actions such as uploading local files. As a result, attackers could make a logged-in administrator upload arbitrary local files via a CSRF attack and send them to the attacker. **CVE ID : CVE-2021-41764**	N/A	A-STR-STRE-061021/314
stylemixthemes					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ulisting					
Authorization Bypass Through User-Controlled Key	27-Sep-21	6.5	Authenticated Insecure Direct Object References (IDOR) vulnerability in WordPress uListing plugin (versions <= 2.0.5). **CVE ID : CVE-2021-36874**	https://wordpress.org/plugins/ulisting/#developers	A-STY-ULIS-061021/315
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	3.5	Authenticated Reflected Cross-Site Scripting (XSS) vulnerability in WordPress uListing plugin (versions <= 2.0.5). Vulnerable parameters: &filter[id], &filter[user], &filter[expired_date], &filter[created_date], &filter[updated_date]. **CVE ID : CVE-2021-36875**	https://wordpress.org/plugins/ulisting/#developers	A-STY-ULIS-061021/316
Cross-Site Request Forgery (CSRF)	27-Sep-21	6.8	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in WordPress uListing plugin (versions <= 2.0.5) as it lacks CSRF checks on plugin administration pages. **CVE ID : CVE-2021-36876**	https://wordpress.org/plugins/ulisting/#developers	A-STY-ULIS-061021/317
Cross-Site Request Forgery (CSRF)	27-Sep-21	4.3	Cross-Site Request Forgery (CSRF) vulnerability in WordPress uListing plugin (versions <= 2.0.5) makes it possible for attackers to modify user roles. **CVE ID : CVE-2021-36877**	https://wordpress.org/plugins/ulisting/#developers	A-STY-ULIS-061021/318
Improper Privilege Management	27-Sep-21	7.5	Unauthenticated Privilege Escalation vulnerability in WordPress uListing plugin (versions <= 2.0.5). Possible if WordPress configuration	https://wordpress.org/plugins/ulisting/#developers	A-STY-ULIS-061021/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows user registration. **CVE ID : CVE-2021-36879**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Sep-21	7.5	Unauthenticated SQL Injection (SQLi) vulnerability in WordPress uListing plugin (versions <= 2.0.3), vulnerable parameter: custom. **CVE ID : CVE-2021-36880**	https://wordpress.org/plugins/ulisting/#developers	A-STY-ULIS-061021/320
surelinesystems					
sureedge_migrator					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-21	7.5	A SQL injection vulnerability exists in Sureline SUREedge Migrator 7.0.7.29360. **CVE ID : CVE-2021-38303**	N/A	A-SUR-SURE-061021/321
Swftools					
swftools					
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function grealloc() located in gmem.cc. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39553**	N/A	A-SWF-SWFT-061021/322
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function Lexer::Lexer() located in Lexer.cc. It allows an attacker	N/A	A-SWF-SWFT-061021/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to cause Denial of Service. **CVE ID : CVE-2021-39554**		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function InfoOutputDev::type3D0() located in InfoOutputDev.cc. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39555**	N/A	A-SWF-SWFT-061021/324
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function InfoOutputDev::type3D1() located in InfoOutputDev.cc. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39556**	N/A	A-SWF-SWFT-061021/325
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function copyString() located in gmem.cc. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39557**	N/A	A-SWF-SWFT-061021/326
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function VectorGraphicOutputDev::drawGeneralImage() located in VectorGraphicOutputDev.cc. It allows an attacker to cause code Execution.	N/A	A-SWF-SWFT-061021/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39558		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function GString::~GString() located in GString.cc. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39559**	N/A	A-SWF-SWFT-061021/328
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function Gfx::opSetFillColorN() located in Gfx.cc. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-39561**	N/A	A-SWF-SWFT-061021/329
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function FileStream::makeSubStream() located in Stream.cc. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39562**	N/A	A-SWF-SWFT-061021/330
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_DumpActions() located in swfaction.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39563**	N/A	A-SWF-SWFT-061021/331
Out-of-bounds	20-Sep-21	6.8	An issue was discovered in swftools through 20200710.	N/A	A-SWF-SWFT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			A heap-buffer-overflow exists in the function swf_DumpActions() located in swfaction.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-39564**		061021/332
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function OpAdvance() located in swfaction.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-39569**	N/A	A-SWF-SWFT-061021/333
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function pool_read() located in pool.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-39574**	N/A	A-SWF-SWFT-061021/334
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function dump_method() located in abc.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39575**	N/A	A-SWF-SWFT-061021/335
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function main() located in swfdump.c. It allows an attacker to cause code Execution.	N/A	A-SWF-SWFT-061021/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39577		
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function string_hash() located in q.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-39579**	N/A	A-SWF-SWFT-061021/337
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function swf_GetPlaceObject() located in swfobject.c. It allows an attacker to cause code Execution. **CVE ID : CVE-2021-39582**	N/A	A-SWF-SWFT-061021/338
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function pool_lookup_string2() located in pool.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39583**	N/A	A-SWF-SWFT-061021/339
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function namespace_set_hash() located in pool.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39584**	N/A	A-SWF-SWFT-061021/340
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference	N/A	A-SWF-SWFT-061021/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exists in the function traits_dump() located in abc.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39585**		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_DumpABC() located in abc.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39587**	N/A	A-SWF-SWFT-061021/342
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_ReadABC() located in abc.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39588**	N/A	A-SWF-SWFT-061021/343
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function parse_metadata() located in abc.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39589**	N/A	A-SWF-SWFT-061021/344
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function params_dump() located in abc.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39590**	N/A	A-SWF-SWFT-061021/345
NULL	20-Sep-21	4.3	An issue was discovered in	N/A	A-SWF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			swftools through 20200710. A NULL pointer dereference exists in the function swf_GetShapeBoundingBox() located in swfshape.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39591**		SWFT-061021/346
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function pool_lookup_uint() located in pool.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39592**	N/A	A-SWF-SWFT-061021/347
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_FontExtract_DefineFontInfo() located in swftext.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39593**	N/A	A-SWF-SWFT-061021/348
NULL Pointer Dereference	20-Sep-21	4.3	Other An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function updateusage() located in swftext.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39594**	N/A	A-SWF-SWFT-061021/349
Out-of-bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function rfx_alloc() located in mem.c.	N/A	A-SWF-SWFT-061021/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			It allows an attacker to cause code Execution. **CVE ID : CVE-2021-39595**		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function code_parse() located in code.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39596**	N/A	A-SWF-SWFT-061021/351
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function code_dump2() located in code.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39597**	N/A	A-SWF-SWFT-061021/352
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function callcode() located in code.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2021-39598**	N/A	A-SWF-SWFT-061021/353
taro					
taro					
N/A	17-Sep-21	7.8	taro is vulnerable to Inefficient Regular Expression Complexity **CVE ID : CVE-2021-3804**	https://hunter.dev/bounties/0ebe85e6-cc85-42b8-957e-18d8df277414, https://github.com/nervjs	A-TAR-TARO-061021/354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/taro/commit/acadb6c826ba57f2030a626f1de4f7b4608fcdb5	
telefication					
telefication					
Server-Side Request Forgery (SSRF)	22-Sep-21	5	The Telefication WordPress plugin is vulnerable to Open Proxy and Server-Side Request Forgery via the ~/bypass.php file due to a user-supplied URL request value that gets called by a curl requests. This affects versions up to, and including, 1.8.0. **CVE ID : CVE-2021-39339**	N/A	A-TEL-TELE-061021/355
thinktwit_project					
thinktwit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The ThinkTwit WordPress plugin before 1.7.1 did not sanitise or escape its "Consumer key" setting before outputting it its settings page, leading to a Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24582**	N/A	A-THI-THIN-061021/356
Torproject					
tor_browser					
Insertion of Sensitive Information into Log File	24-Sep-21	3.6	Tor Browser through 10.5.6 and 11.x through 11.0a4 allows a correlation attack that can compromise the privacy of visits to v2 onion addresses. Exact timestamps	https://gitlab.torproject.org/tpo/core/tor/-/commit/80c404c4b79f3	A-TOR-TOR_-061021/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of these onion-service visits are logged locally, and an attacker might be able to compare them to timestamp data collected by the destination server (or collected by a rogue site within the Tor network). **CVE ID : CVE-2021-39246**	bcba3fc4585d4c62a62a04f3ed9, https://gitlab.torproject.org/tpo/core/tor/-/merge_requests/434	
Trendmicro					
housecall_for_home_networks					
Uncontrolled Search Path Element	29-Sep-21	6.9	An uncontrolled search path element privilege escalation vulnerability in Trend Micro HouseCall for Home Networks version 5.3.1225 and below could allow an attacker to escalate privileges by placing a custom crafted file in a specific directory to load a malicious library. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability. **CVE ID : CVE-2021-32466**	https://helpcenter.trendmicro.com/ja-jp/article/TMKA-10621, https://helpcenter.trendmicro.com/en-us/article/tmka-10626	A-TRE-HOUS-061021/358
serverprotect					
Improper Authentication	29-Sep-21	10	A vulnerability in Trend Micro ServerProtect for Storage 6.0, ServerProtect for EMC Celerra 5.8, ServerProtect for Network Appliance Filers 5.8, and ServerProtect for Microsoft Windows / Novell Netware 5.8 could allow a remote attacker to bypass authentication on affected	https://success.trendmicro.com/solution/000289038, https://success.trendmicro.com/jp/solution/000289030	A-TRE-SERV-061021/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installations. **CVE ID : CVE-2021-36745**		
tubitak					
pardus_software_center					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Sep-21	7.1	A path traversal vulnerability on Pardus Software Center's "extractArchive" function could allow anyone on the same network to do a man-in-the-middle and write files on the system. **CVE ID : CVE-2021-3806**	https://pentest.blog/pardus-21-linux-distro-remote-code-execution-0day-2021/, https://www.usom.gov.tr/bildirim/tr-21-0754	A-TUB-PARD-061021/360
ui					
unifi_talk					
Improper Control of Generation of Code ('Code Injection')	23-Sep-21	6.5	A vulnerability found in UniFi Talk application V1.12.3 and earlier permits a malicious actor who has already gained access to a network to subsequently control Talk device(s) assigned to said network if they are not yet adopted. This vulnerability is fixed in UniFi Talk application V1.12.5 and later. **CVE ID : CVE-2021-22952**	N/A	A-UI-UNIF-061021/361
Vmware					
cloud_foundation					
Server-Side Request Forgery (SSRF)	23-Sep-21	4	The vCenter Server contains an SSRF (Server Side Request Forgery) vulnerability due to improper validation of URLs in vCenter Server Content	https://www.vmware.com/security/advisories/VMSA-2021-	A-VMW-CLOU-061021/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Library. An authorised user with access to content library may exploit this issue by sending a POST request to vCenter Server leading to information disclosure. **CVE ID : CVE-2021-21993**	0020.html	
Unrestricted Upload of File with Dangerous Type	23-Sep-21	7.5	The vCenter Server contains an arbitrary file upload vulnerability in the Analytics service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to execute code on vCenter Server by uploading a specially crafted file. **CVE ID : CVE-2021-22005**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/363
N/A	23-Sep-21	5	The vCenter Server contains a reverse proxy bypass vulnerability due to the way the endpoints handle the URI. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to access restricted endpoints. **CVE ID : CVE-2021-22006**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/364
Exposure of Resource to Wrong Sphere	23-Sep-21	2.1	The vCenter Server contains a local information disclosure vulnerability in the Analytics service. An authenticated user with non-administrative privilege may exploit this issue to gain access to sensitive information. **CVE ID : CVE-2021-22007**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/365
Exposure of Resource to	23-Sep-21	5	The vCenter Server contains an information disclosure	https://www.vmware.co	A-VMW-CLOU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			vulnerability in VAPI (vCenter API) service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue by sending a specially crafted json-rpc message to gain access to sensitive information. **CVE ID : CVE-2021-22008**	m/security/advisories/VMSA-2021-0020.html	061021/366
Uncontrolled Resource Consumption	23-Sep-21	5	The vCenter Server contains multiple denial-of-service vulnerabilities in VAPI (vCenter API) service. A malicious actor with network access to port 443 on vCenter Server may exploit these issues to create a denial of service condition due to excessive memory consumption by VAPI service. **CVE ID : CVE-2021-22009**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/367
Uncontrolled Resource Consumption	23-Sep-21	5	The vCenter Server contains a denial-of-service vulnerability in VPXD service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to create a denial of service condition due to excessive memory consumption by VPXD service. **CVE ID : CVE-2021-22010**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/368
N/A	23-Sep-21	5	vCenter Server contains an unauthenticated API endpoint vulnerability in vCenter Server Content Library. A malicious actor	https://www.vmware.com/security/advisories/VMSA-2021-	A-VMW-CLOU-061021/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with network access to port 443 on vCenter Server may exploit this issue to perform unauthenticated VM network setting manipulation. **CVE ID : CVE-2021-22011**	0020.html	
Exposure of Resource to Wrong Sphere	23-Sep-21	5	The vCenter Server contains an information disclosure vulnerability due to an unauthenticated appliance management API. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information. **CVE ID : CVE-2021-22012**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/370
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Sep-21	5	The vCenter Server contains a file path traversal vulnerability leading to information disclosure in the appliance management API. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information. **CVE ID : CVE-2021-22013**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/371
N/A	23-Sep-21	9	The vCenter Server contains an authenticated code execution vulnerability in VAMI (Virtual Appliance Management Infrastructure). An authenticated VAMI user with network access to port 5480 on vCenter Server may exploit this issue to execute code on the underlying operating system that hosts	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vCenter Server. **CVE ID : CVE-2021-22014**		
Improper Privilege Management	23-Sep-21	7.2	The vCenter Server contains multiple local privilege escalation vulnerabilities due to improper permissions of files and directories. An authenticated local user with non-administrative privilege may exploit these issues to elevate their privileges to root on vCenter Server Appliance. **CVE ID : CVE-2021-22015**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/373
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	4.3	The vCenter Server contains a reflected cross-site scripting vulnerability due to a lack of input sanitization. An attacker may exploit this issue to execute malicious scripts by tricking a victim into clicking a malicious link. **CVE ID : CVE-2021-22016**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/374
N/A	23-Sep-21	6.4	The vCenter Server contains an arbitrary file deletion vulnerability in a VMware vSphere Life-cycle Manager plug-in. A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete non critical files. **CVE ID : CVE-2021-22018**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/375
N/A	23-Sep-21	5	The vCenter Server contains a denial-of-service vulnerability in VAPI (vCenter API) service. A malicious actor with network access to port 5480 on	https://www.vmware.com/security/advisories/VMSA-2021-	A-VMW-CLOU-061021/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vCenter Server may exploit this issue by sending a specially crafted jsonrpc message to create a denial of service condition. **CVE ID : CVE-2021-22019**	0020.html	
N/A	23-Sep-21	2.1	The vCenter Server contains a denial-of-service vulnerability in the Analytics service. Successful exploitation of this issue may allow an attacker to create a denial-of-service condition on vCenter Server. **CVE ID : CVE-2021-22020**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-CLOU-061021/377
vcenter_server					
Server-Side Request Forgery (SSRF)	23-Sep-21	4	The vCenter Server contains an SSRF (Server Side Request Forgery) vulnerability due to improper validation of URLs in vCenter Server Content Library. An authorised user with access to content library may exploit this issue by sending a POST request to vCenter Server leading to information disclosure. **CVE ID : CVE-2021-21993**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/378
Unrestricted Upload of File with Dangerous Type	23-Sep-21	7.5	The vCenter Server contains an arbitrary file upload vulnerability in the Analytics service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to execute code on vCenter Server by uploading a specially crafted file.	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22005		
N/A	23-Sep-21	5	The vCenter Server contains a reverse proxy bypass vulnerability due to the way the endpoints handle the URI. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to access restricted endpoints. **CVE ID : CVE-2021-22006**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/380
Exposure of Resource to Wrong Sphere	23-Sep-21	2.1	The vCenter Server contains a local information disclosure vulnerability in the Analytics service. An authenticated user with non-administrative privilege may exploit this issue to gain access to sensitive information. **CVE ID : CVE-2021-22007**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/381
Exposure of Resource to Wrong Sphere	23-Sep-21	5	The vCenter Server contains an information disclosure vulnerability in VAPI (vCenter API) service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue by sending a specially crafted json-rpc message to gain access to sensitive information. **CVE ID : CVE-2021-22008**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/382
Uncontrolled Resource Consumption	23-Sep-21	5	The vCenter Server contains multiple denial-of-service vulnerabilities in VAPI (vCenter API) service. A malicious actor with network access to port 443 on vCenter Server may exploit these	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issues to create a denial of service condition due to excessive memory consumption by VAPI service. **CVE ID : CVE-2021-22009**		
Uncontrolled Resource Consumption	23-Sep-21	5	The vCenter Server contains a denial-of-service vulnerability in VPXD service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to create a denial of service condition due to excessive memory consumption by VPXD service. **CVE ID : CVE-2021-22010**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/384
N/A	23-Sep-21	5	vCenter Server contains an unauthenticated API endpoint vulnerability in vCenter Server Content Library. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to perform unauthenticated VM network setting manipulation. **CVE ID : CVE-2021-22011**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/385
Exposure of Resource to Wrong Sphere	23-Sep-21	5	The vCenter Server contains an information disclosure vulnerability due to an unauthenticated appliance management API. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information. **CVE ID : CVE-2021-22012**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Sep-21	5	The vCenter Server contains a file path traversal vulnerability leading to information disclosure in the appliance management API. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information. **CVE ID : CVE-2021-22013**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/387
N/A	23-Sep-21	9	The vCenter Server contains an authenticated code execution vulnerability in VAMI (Virtual Appliance Management Infrastructure). An authenticated VAMI user with network access to port 5480 on vCenter Server may exploit this issue to execute code on the underlying operating system that hosts vCenter Server. **CVE ID : CVE-2021-22014**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/388
Improper Privilege Management	23-Sep-21	7.2	The vCenter Server contains multiple local privilege escalation vulnerabilities due to improper permissions of files and directories. An authenticated local user with non-administrative privilege may exploit these issues to elevate their privileges to root on vCenter Server Appliance. **CVE ID : CVE-2021-22015**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/389
Improper Neutralization of Input	23-Sep-21	4.3	The vCenter Server contains a reflected cross-site scripting vulnerability due to a lack of	https://www.vmware.com/security/a	A-VMW-VCEN-061021/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			input sanitization. An attacker may exploit this issue to execute malicious scripts by tricking a victim into clicking a malicious link. **CVE ID : CVE-2021-22016**	dvisories/VMSA-2021-0020.html	
N/A	23-Sep-21	5	Rhttproxy as used in vCenter Server contains a vulnerability due to improper implementation of URI normalization. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to bypass proxy leading to internal endpoints being accessed. **CVE ID : CVE-2021-22017**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/391
N/A	23-Sep-21	6.4	The vCenter Server contains an arbitrary file deletion vulnerability in a VMware vSphere Life-cycle Manager plug-in. A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete non critical files. **CVE ID : CVE-2021-22018**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/392
N/A	23-Sep-21	5	The vCenter Server contains a denial-of-service vulnerability in VAPI (vCenter API) service. A malicious actor with network access to port 5480 on vCenter Server may exploit this issue by sending a specially crafted jsonrpc message to create a denial of service condition.	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22019		
N/A	23-Sep-21	2.1	The vCenter Server contains a denial-of-service vulnerability in the Analytics service. Successful exploitation of this issue may allow an attacker to create a denial-of-service condition on vCenter Server. **CVE ID : CVE-2021-22020**	https://www.vmware.com/security/advisories/VMSA-2021-0020.html	A-VMW-VCEN-061021/394
wbolt					
donate_with_qrcode					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The Donate With QRCode WordPress plugin before 1.4.5 does not sanitise or escape its QRCode Image setting, which result into a Stored Cross-Site Scripting (XSS). Furthermore, the plugin also does not have any CSRF and capability checks in place when saving such setting, allowing any authenticated user (as low as subscriber), or unauthenticated user via a CSRF vector to update them and perform such attack. **CVE ID : CVE-2021-24618**	N/A	A-WBO-DONA-061021/395
webence					
iq_block_country					
Improper Neutralization of Input During Web Page Generation ('Cross-site	23-Sep-21	3.5	Authenticated Persistent Cross-Site Scripting (XSS) vulnerability in WordPress iQ Block Country plugin (versions <= 1.2.11). Vulnerable parameter: &blockcountry_blockmessage	https://wordpress.org/plugins/iq-block-country/#developers	A-WEB-IQ_B-061021/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			. **CVE ID : CVE-2021-36873**		
webpsilon					
responsive_3d_slider					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The Add new scene functionality in the Responsive 3D Slider WordPress plugin through 1.2 uses an id parameter which is not sanitised, escaped or validated before being inserted to a SQL statement, leading to SQL injection. This is a time based SQLI and in the same function vulnerable parameter is passed twice so if we pass time as 5 seconds it takes 10 seconds to return since the query is ran twice. **CVE ID : CVE-2021-24398**	N/A	A-WEB-RESP-061021/397
weseek					
growi					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-21	4.3	Cross-site scripting vulnerability due to the inadequate tag sanitization in GROWI versions v4.2.19 and earlier allows remote attackers to execute an arbitrary script on the web browser of the user who accesses a specially crafted page. **CVE ID : CVE-2021-20829**	https://weseek.co.jp/security/2021/09/17/vulnerability/growi-prevent-multiple-xss-addition/	A-WES-GROW-061021/398
wordpress_popular_posts_project					
wordpress_popular_posts					
Improper	23-Sep-21	3.5	Authenticated Persistent	https://githu	A-WOR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting (XSS) vulnerability in WordPress Popular Posts plugin (versions <= 5.3.3). Vulnerable at &widget-wpp[2][post_type]. **CVE ID : CVE-2021-36872**	b.com/cabrerahector/wordpress-popular-posts/blob/master/changelog.md	WORD-061021/399
wp-board_project					
wp-board					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The options.php file of the WP-Board WordPress plugin through 1.1 beta accepts a postid parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. This is a time based SQLI and in the same function vulnerable parameter is passed twice so if we pass time as 5 seconds it takes 10 seconds to return since the query ran twice. **CVE ID : CVE-2021-24404**	N/A	A-WP--WP-B-061021/400
wp-domain-redirect_project					
wp-domain-redirect					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The Edit domain functionality in the WP Domain Redirect WordPress plugin through 1.0 has an `editid` parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. **CVE ID : CVE-2021-24401**	N/A	A-WP--WP-D-061021/401
wpagecontact_project					
wpagecontact					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The Orders functionality in the WordPress Page Contact plugin through 1.0 has an order_id parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. The feature is available to low privilege users such as contributors **CVE ID : CVE-2021-24403**	N/A	A-WPA-WPAG-061021/402
wpdevart					
countdown_and_countup\\,_woocommerce_sales_timer					
Cross-Site Request Forgery (CSRF)	28-Sep-21	6.8	The Countdown and CountUp, WooCommerce Sales Timers WordPress plugin is vulnerable to Cross-Site Request Forgery via the save_theme function found in the ~/includes/admin/coundown_theme_page.php file due to a missing nonce check which allows attackers to inject arbitrary web scripts, in versions up to and including 1.5.7. **CVE ID : CVE-2021-34636**	https://plugins.trac.wordpress.org/changeset/2605523/countdown-wpdevart-extended/trunk/includes/admin/coundown_theme_page.php	A-WPD-COUN-061021/403
wpxpo					
postx_-_gutenberg_blocks_for_post_grid					
Incorrect Authorization	27-Sep-21	4	The PostX â€“ Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10 performs incorrect checks before allowing any logged in user to perform some ajax based requests, allowing any user to modify,	N/A	A-WPX-POST-061021/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delete or add ultp_options values. **CVE ID : CVE-2021-24652**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	3.5	The PostX â€“ Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10 allows users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks via the plugin's block. **CVE ID : CVE-2021-24659**	N/A	A-WPX-POST-061021/405
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	3.5	The PostX â€“ Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10, with Saved Templates Addon enabled, allows users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks via the plugin's shortcode. **CVE ID : CVE-2021-24660**	N/A	A-WPX-POST-061021/406
Exposure of Sensitive Information to an Unauthorized Actor	27-Sep-21	3.5	The PostX â€“ Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10, with Saved Templates Addon enabled, allows users with Contributor roles or higher to read password-protected or private post contents the user is otherwise unable to read, given the post ID. **CVE ID : CVE-2021-24661**	N/A	A-WPX-POST-061021/407
wp_dialog_project					
wp_dialog					
Improper	20-Sep-21	3.5	The WP Dialog WordPress	N/A	A-WP_-WP_D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			plugin through 1.2.5.5 does not sanitise and escape some of its settings before outputting them in pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24600**		061021/408
wp_mapa_politico_espana_project					
wp_mapa_politico_espana					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The WP Mapa Politico Espana WordPress plugin before 3.7.0 does not sanitise or escape some of its settings before outputting them in attributes, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed **CVE ID : CVE-2021-24609**	N/A	A-WP_-WP_M-061021/409
wuzhicms					
wuzhicms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-21	7.5	SQL Injection vulnerability exists in Wuzhi CMS 4.1.0 via the keywords parameter under the coreframe/app/promote/admin/index.php file. **CVE ID : CVE-2021-40669**	N/A	A-WUZ-WUZH-061021/410
Improper Neutralization of Special Elements	16-Sep-21	7.5	SQL Injection vulnerability exists in Wuzhi CMS 4.1.0 via the keywords iparameter under the	N/A	A-WUZ-WUZH-061021/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			/coreframe/app/order/admin/card.php file. **CVE ID : CVE-2021-40670**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	7.5	An SQL injection vulnerability exists in Wuzhi CMS v4.1.0 via the KeyValue parameter in coreframe/app/order/admin/index.php. **CVE ID : CVE-2021-40674**	N/A	A-WUZ-WUZH-061021/412
xfig_project					
fig2dev					
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in fig2dev before 3.2.8.. A NULL pointer dereference exists in the function compute_closed_spline() located in trans_spline.c. It allows an attacker to cause Denial of Service. The fixed version of fig2dev is 3.2.8. **CVE ID : CVE-2021-32280**	https://sourceforge.net/p/mcj/tickets/107/, https://sourceforge.net/p/mcj/fig2dev/ci/f17a3b8a7d54c1bc56ab92512531772a0b3ec991/	A-XFI-FIG2-061021/413
xss_hunter_express_project					
xss_hunter_express					
Improper Authentication	17-Sep-21	7.5	XSS Hunter Express before 2021-09-17 does not properly enforce authentication requirements for paths. **CVE ID : CVE-2021-41317**	https://github.com/mandatoryprogrammer/xsshunter-express/commit/56bb44ed9024849f64173f71583	A-XSS-XSS_-061021/414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ecb7d873baba0	
yithemes					
yith_maintenance_mode					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	3.5	Authenticated Stored Cross-Site Scripting (XSS) vulnerability in YITH Maintenance Mode (WordPress plugin) versions <= 1.3.7, vulnerable parameter &yith_maintenance_newsletter_submit_label. Possible even when unfiltered HTML is disallowed by WordPress configuration. **CVE ID : CVE-2021-36841**	https://wordpress.org/plugins/yith-maintenance-mode/#developers	A-YIT-YITH-061021/415
you-shang_project					
you-shang					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The You Shang WordPress plugin through 1.0.1 does not escape its qrcode links settings, which result into Stored Cross-Site Scripting issues in frontend posts and the plugins settings page depending on the payload used **CVE ID : CVE-2021-24597**	N/A	A-YOU-YOU--061021/416
zeesweb					
splash_header					
Improper Neutralization of Input During Web Page Generation	20-Sep-21	3.5	The Splash Header WordPress plugin before 1.20.8 doesn't sanitise and escape some of its settings while outputting them in the admin dashboard, leading to	N/A	A-ZEE-SPLA-061021/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			an authenticated Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24587**		
Zohocorp					
manageengine_admanager_plus					
Server-Side Request Forgery (SSRF)	21-Sep-21	7.5	ManageEngine ADSelfService Plus before 6112 is vulnerable to SSRF. **CVE ID : CVE-2021-37419**	https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6112-hotfix-release	A-ZOH-MANA-061021/418
Improper Authentication	21-Sep-21	5	ManageEngine ADSelfService Plus before 6112 is vulnerable to mail spoofing. **CVE ID : CVE-2021-37420**	https://www.manageengine.com, https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6112-hotfix-release	A-ZOH-MANA-061021/419
Improper Privilege Management	21-Sep-21	7.5	ManageEngine ADSelfService Plus before 6112 is vulnerable to domain user account takeover. **CVE ID : CVE-2021-37424**	https://www.manageengine.com, https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6112-hotfix-release	A-ZOH-MANA-061021/420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	27-Sep-21	7.5	Zoho ManageEngine ADManager Plus before 7111 is vulnerable to unrestricted file which leads to Remote code execution. **CVE ID : CVE-2021-37539**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-061021/421
Improper Authentication	21-Sep-21	6.5	ManageEngine ADManager Plus before 7111 has Pre-authentication RCE vulnerabilities. **CVE ID : CVE-2021-37741**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111, https://www.manageengine.com	A-ZOH-MANA-061021/422
Unrestricted Upload of File with Dangerous Type	27-Sep-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior is vulnerable to unrestricted file upload, leading to remote code execution. **CVE ID : CVE-2021-37761**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-061021/423
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Sep-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior has a Post-Auth OS command injection vulnerability. **CVE ID : CVE-2021-37925**	https://www.manageengine.com/products/ad-manager/release-notes.html#7111	A-ZOH-MANA-061021/424
Improper Authentication	22-Sep-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows	https://www.manageengine.com/products/ad-	A-ZOH-MANA-061021/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			account takeover via SSO. **CVE ID : CVE-2021-37927**	manager/release-notes.html#7111	
ZTE					
axon_30_pro_message_service					
N/A	25-Sep-21	4.3	There is an information leak vulnerability in the message service app of a ZTE mobile phone. Due to improper parameter settings, attackers could use this vulnerability to obtain some sensitive information of users by accessing specific pages. **CVE ID : CVE-2021-21742**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019084	A-ZTE-AXON-061021/426
Hardware					
Cisco					
1100-8p					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-1100-061021/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
1120					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-1120-061021/428
1160					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-1160-061021/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
7600_router					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	H-CIS-7600-061021/430
aironet_1542d					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/431
aironet_1542i					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_1562d					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/433
aironet_1562e					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_1562i					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/435
aironet_1815i					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points	https://tools.cisco.com/security/center	H-CIS-AIRO-061021/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	
aironet_1815m					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_1815t					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/438
aironet_1815w					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_1830e					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/440
aironet_1830i					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-AIRO-061021/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	sa-cisco-ap-LLjsGxv	
aironet_1840i					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
aironet_1850e					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/443
aironet_1850i					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_2800e					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/445
aironet_2800i					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_3800e					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/447
aironet_3800i					
Improper Privilege	23-Sep-21	7.2	A vulnerability in the SSH management feature of	https://tools.cisco.com/se	H-CIS-AIRO-061021/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	
aironet_3800p					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_4800					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-AIRO-061021/450
asr_1000-x					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ASR_-061021/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**		
asr_1001					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ASR_-061021/452
asr_1001-x					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAd	H-CIS-ASR_-061021/453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	visory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	
asr_1002					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ASR_-061021/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
asr_1002-x					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ASR_-061021/455
asr_1004					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ASR_-061021/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**		
asr_1006					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ASR_-061021/457
asr_1013					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-	H-CIS-ASR_-061021/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	MVOF3ZZn	
asr_1023					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ASR_-061021/459
asr_901-12c-f-d					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service	https://tools.cisco.com/se	H-CIS-ASR_-061021/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	
asr_901-12c-ft-d					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	H-CIS-ASR_-061021/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**		
asr_901-4c-f-d					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	H-CIS-ASR_-061021/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1622		
asr_901-4c-ft-d					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	H-CIS-ASR_-061021/463
asr_901-6cz-f-a					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	H-CIS-ASR_-061021/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**		
asr_901-6cz-f-d					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	H-CIS-ASR_-061021/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**		
asr_901-6cz-fs-a					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	H-CIS-ASR_-061021/466
asr_901-6cz-fs-d					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8	https://tools.cisco.com/security/center/content/Cis	H-CIS-ASR_-061021/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**	coSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	
asr_901-6cz-ft-a					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	H-CIS-ASR_-061021/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**		
asr_901-6cz-ft-d					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	H-CIS-ASR_-061021/469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
catalyst_9105					
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP. **CVE ID : CVE-2021-1615**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ewc-dos-g6JruHRT	H-CIS-CATA-061021/470
catalyst_9105axi					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_9105axw					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/472
catalyst_9115					
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ewc-dos-	H-CIS-CATA-061021/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP. **CVE ID : CVE-2021-1615**	g6JruHRT	
catalyst_9115axe					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/474
catalyst_9115axi					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/475
catalyst_9117					
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ewc-dos-g6JruHRT	H-CIS-CATA-061021/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP. **CVE ID : CVE-2021-1615**		
catalyst_9117axi					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/477
catalyst_9120					
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ewc-dos-g6JruHRT	H-CIS-CATA-061021/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP. **CVE ID : CVE-2021-1615**		
catalyst_9120axe					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/479
catalyst_9120axi					
Improper	23-Sep-21	7.2	A vulnerability in the SSH	https://tools.	H-CIS-CATA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	061021/480
catalyst_9120axp					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_9124					
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP. **CVE ID : CVE-2021-1615**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ewc-dos-g6JruHRT	H-CIS-CATA-061021/482
catalyst_9124axd					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_9124axi					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/484
catalyst_9130					
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless	https://tools.cisco.com/security/center	H-CIS-CATA-061021/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP. **CVE ID : CVE-2021-1615**	/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ewc-dos-g6JruHRT	
catalyst_9130axe					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_9130axi					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/487
catalyst_9800-40					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_9800-80					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/489
catalyst_9800-cl					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to	https://tools.cisco.com/security/center/content/CiscoSecurityAd	H-CIS-CATA-061021/490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	visory/cisco-sa-cisco-ap-LLjsGxv	
catalyst_9800-l					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
catalyst_iw6300_ac					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/492
catalyst_iw6300_dc					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_iw6300_dcw					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/494
cbr-8					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbr8-cops-Vc2ZsJSx	H-CIS-CBR--061021/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. **CVE ID : CVE-2021-1622**		
csr1000v					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-CSR1-061021/496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34723		
esw-6300					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	H-CIS-ESW--061021/497
isr1100					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ISR1-061021/498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**		
isr1100-4g					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ISR1-061021/499
isr1100-4gltegb					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-ISR1-061021/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	iosxesdwan-arbfileov-MVOF3ZZn	
isr1100-4gltena					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ISR1-061021/501
isr1100-6g					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ISR1-061021/502
isr1100-lte					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ISR1-061021/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**		
isr_4321					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ISR_-061021/504
isr_4331					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ISR_-061021/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**		
isr_4351					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ISR_-061021/506
isr_4431					
Exposure of Resource to Wrong	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN	https://tools.cisco.com/security/center	H-CIS-ISR_-061021/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	
vedge_100					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	H-CIS-VEDG-061021/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vedge_1000					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	H-CIS-VEDG-061021/509
vedge_100b					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	H-CIS-VEDG-061021/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1546		
vedge_100m					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	H-CIS-VEDG-061021/511
vedge_100wm					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	H-CIS-VEDG-061021/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive information. **CVE ID : CVE-2021-1546**		
vedge_2000					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	H-CIS-VEDG-061021/513
vedge_5000					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	H-CIS-VEDG-061021/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**		
vedge_cloud					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	H-CIS-VEDG-061021/515
vsmart_controller					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	H-CIS-VSMA-061021/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**		
D-link					
dcs-5000l					
Improper Authenticati on	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** DCS-5000L v1.05 and DCS-932L v2.17 and older are affecged by Incorrect Acess Control. The use of the basic authentication for the devices command interface allows attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-41503**	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10247	H-D-L-DCS--061021/517
Improper Privilege Management	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** An Elevated Privileges issue exists in D-Link DCS-5000L v1.05 and DCS-932L v2.17 and older. The use of the digest-authentication for the devices command interface may allow further attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10247	H-D-L-DCS--061021/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			maintainer. **CVE ID : CVE-2021-41504**		
dcs-932l					
Improper Authenticati on	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** DCS-5000L v1.05 and DCS-932L v2.17 and older are affecged by Incorrect Acess Control. The use of the basic authentication for the devices command interface allows attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-41503**	https://ww w.dlink.com/ en/security-bulletin/, https://supp ortannounce ment.us.dlin k.com/annou ncement/pu blication.asp x?name=SAP 10247	H-D-L-DCS--061021/519
Improper Privilege Management	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** An Elevated Privileges issue exists in D-Link DCS-5000L v1.05 and DCS-932L v2.17 and older. The use of the digest-authentication for the devices command interface may allow further attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-41504**	https://ww w.dlink.com/ en/security-bulletin/, https://supp ortannounce ment.us.dlin k.com/annou ncement/pu blication.asp x?name=SAP 10247	H-D-L-DCS--061021/520
Dlink					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dir-3040					
Use of Hard-coded Credentials	23-Sep-21	7.5	An information disclosure vulnerability exists in the WiFi Smart Mesh functionality of D-LINK DIR-3040 1.13B03. A specially-crafted network request can lead to command execution. An attacker can connect to the MQTT service to trigger this vulnerability. **CVE ID : CVE-2021-21913**	N/A	H-DLI-DIR--061021/521
dir-605l					
Insufficiently Protected Credentials	24-Sep-21	5	An informtion disclosure issue exists in D-LINK-DIR-605 B2 Firmware Version : 2.01MT. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page **CVE ID : CVE-2021-40655**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--061021/522
dir-615					
Insufficiently Protected Credentials	24-Sep-21	4	An information disclosure issue exist in D-LINK-DIR-615 B2 2.01mt. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page **CVE ID : CVE-2021-40654**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--061021/523
kadenvodomery					
picoflux_air					
Observable Discrepancy	16-Sep-21	3.3	In Kaden PICOFLUX Air in all known versions an information exposure through observable	https://www.fit.vutbr.cz/~polcak/CVE-2021-	H-KAD-PICO-061021/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			discrepancy exists. This may give sensitive information (water consumption without distinct values) to third parties. **CVE ID : CVE-2021-34576**	34576.en	
mediatek					
mt6580					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/525
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/526
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/528
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/529
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810. **CVE ID : CVE-2021-0611**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/531
mt6582e					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/532
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/534
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/535
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/536
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT65-061021/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	security-bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/538
mt6582h					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/539
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/541
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/542
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456. **CVE ID : CVE-2021-0610**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/544
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/545
mt6582t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/546
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	mediatek.com/product-security-bulletin/September-2021	MT65-061021/547
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/548
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/549
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp.mediatek.com/product-security-	H-MED-MT65-061021/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/551
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/552
mt6582w					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/554
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/555
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/557
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/558
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/559
mt6582_90					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp.mediatek.co	H-MED-MT65-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	m/product-security-bulletin/September-2021	061021/560
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/561
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/562
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp.mediatek.com/product-security-bulletin/Sept	H-MED-MT65-061021/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/564
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/565
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834. **CVE ID : CVE-2021-0612**		
mt6589					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/567
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/568
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/570
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/571
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/572
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT65-061021/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	security-bulletin/September-2021	
mt6589td					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/574
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/575
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/577
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/578
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810. **CVE ID : CVE-2021-0611**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/580
mt6592e					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/581
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/583
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/584
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/585
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT65-061021/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	security-bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/587
mt6592h					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/588
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/590
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/591
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456. **CVE ID : CVE-2021-0610**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/593
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/594
mt6592t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/595
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	mediatek.com/product-security-bulletin/September-2021	MT65-061021/596
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/597
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/598
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp.mediatek.com/product-security-	H-MED-MT65-061021/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/600
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/601
mt6592w					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/603
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/604
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/606
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/607
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/608
mt6592_90					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp.mediatek.co	H-MED-MT65-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	m/product-security-bulletin/September-2021	061021/609
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/610
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/611
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp.mediatek.com/product-security-bulletin/Sept	H-MED-MT65-061021/612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/613
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/614
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834. **CVE ID : CVE-2021-0612**		
mt6595					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/616
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/617
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/619
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/620
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT65-061021/621
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT65-061021/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	security-bulletin/September-2021	
mt6731					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/623
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/624
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/626
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/627
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810. **CVE ID : CVE-2021-0611**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/629
mt6732					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/630
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/632
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/633
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/634
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT67-061021/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	security-bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/636
mt6735					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/637
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/639
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/640
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456. **CVE ID : CVE-2021-0610**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/642
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/643
mt6737					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/644
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	mediatek.com/product-security-bulletin/September-2021	MT67-061021/645
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/646
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/647
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-061021/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/649
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/650
mt6739					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/652
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/653
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/655
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/656
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/657
mt6750					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp.mediatek.co	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	m/product-security-bulletin/September-2021	061021/658
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/659
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/660
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp.mediatek.com/product-security-bulletin/Sept	H-MED-MT67-061021/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/662
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/663
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834. **CVE ID : CVE-2021-0612**		
mt6750s					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/665
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/666
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/668
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/669
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/670
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT67-061021/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	security-bulletin/September-2021	
mt6752					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/672
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/673
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/675
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/676
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810. **CVE ID : CVE-2021-0611**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/678
mt6753					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/679
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/681
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/682
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/683
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT67-061021/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	security-bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/685
mt6755					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/686
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/688
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/689
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456. **CVE ID : CVE-2021-0610**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/691
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/692
mt6755s					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/693
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	mediatek.com/product-security-bulletin/September-2021	MT67-061021/694
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/695
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/696
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-061021/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/698
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/699
mt6757					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/701
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/702
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/704
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/705
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/706
mt6757c					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp.mediatek.co	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	m/product-security-bulletin/September-2021	061021/707
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/708
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/709
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp.mediatek.com/product-security-bulletin/Sept	H-MED-MT67-061021/710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/711
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/712
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834. **CVE ID : CVE-2021-0612**		
mt6757cd					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/714
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/715
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/717
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/718
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/719
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT67-061021/720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	security-bulletin/September-2021	
mt6757ch					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/721
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/722
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/724
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/725
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810. **CVE ID : CVE-2021-0611**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/727
mt6758					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/728
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/730
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/731
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/732
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT67-061021/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	security-bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/734
mt6761					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/735
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/737
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/738
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456. **CVE ID : CVE-2021-0610**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/740
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/741
mt6762					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/742
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	mediatek.com/product-security-bulletin/September-2021	MT67-061021/743
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/744
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/745
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-061021/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/747
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/748
mt6763					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/750
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/751
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/753
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/754
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/755
mt6765					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp.mediatek.co	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	m/product-security-bulletin/September-2021	061021/756
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/757
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/758
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp.mediatek.com/product-security-bulletin/Sept	H-MED-MT67-061021/759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/760
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/761
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834. **CVE ID : CVE-2021-0612**		
mt6768					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/763
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/764
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/766
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/767
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/768
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT67-061021/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	security-bulletin/September-2021	
mt6769					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/770
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/771
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/773
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/774
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810. **CVE ID : CVE-2021-0611**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/776
mt6771					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/777
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/779
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/780
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/781
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT67-061021/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	security-bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/783
mt6779					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/784
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/786
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/787
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456. **CVE ID : CVE-2021-0610**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/789
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/790
Out-of-bounds Read	27-Sep-21	4	In ccu, there is a possible out of bounds read due to incorrect error handling. This could lead to information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827145; Issue ID: ALPS05827145. **CVE ID : CVE-2021-0660**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/791
mt6785					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp.mediatek.co	H-MED-MT67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	m/product-security-bulletin/September-2021	061021/792
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/793
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/794
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp.mediatek.com/product-security-bulletin/Sept	H-MED-MT67-061021/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/796
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/797
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834. **CVE ID : CVE-2021-0612**		
mt6795					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/799
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/800
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/802
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/803
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/804
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT67-061021/805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	security-bulletin/September-2021	
mt6797					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/806
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/807
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/809
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/810
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810. **CVE ID : CVE-2021-0611**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/812
mt6799					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/813
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/815
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/816
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/817
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT67-061021/818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	security-bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT67-061021/819
mt6833					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/820
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/822
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/823
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456. **CVE ID : CVE-2021-0610**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/825
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/826
mt6853					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/827
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	mediatek.com/product-security-bulletin/September-2021	MT68-061021/828
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/829
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/830
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-061021/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/832
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/833
Out-of-bounds Read	27-Sep-21	4	In ccu, there is a possible out of bounds read due to incorrect error handling. This could lead to information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827145; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05827145. **CVE ID : CVE-2021-0660**		
mt6853t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/835
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/836
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/838
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/839
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/840
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT68-061021/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	security-bulletin/September-2021	
mt6873					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/842
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/843
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/845
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/846
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810. **CVE ID : CVE-2021-0611**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/848
Out-of-bounds Read	27-Sep-21	4	In ccu, there is a possible out of bounds read due to incorrect error handling. This could lead to information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827145; Issue ID: ALPS05827145. **CVE ID : CVE-2021-0660**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/849
mt6875					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/850
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	mediatek.com/product-security-bulletin/September-2021	MT68-061021/851
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/852
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/853
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-061021/854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/855
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/856
mt6877					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/858
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/859
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/861
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/862
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/863
mt6883					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp.mediatek.co	H-MED-MT68-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	m/product-security-bulletin/September-2021	061021/864
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/865
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/866
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp.mediatek.com/product-security-bulletin/Sept	H-MED-MT68-061021/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/868
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/869
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834. **CVE ID : CVE-2021-0612**		
mt6885					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/871
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/872
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/874
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/875
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/876
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp.mediatek.com/product-	H-MED-MT68-061021/877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	security-bulletin/September-2021	
Out-of-bounds Read	27-Sep-21	4	In ccu, there is a possible out of bounds read due to incorrect error handling. This could lead to information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827145; Issue ID: ALPS05827145. **CVE ID : CVE-2021-0660**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/878
mt6889					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/879
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/881
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/882
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456. **CVE ID : CVE-2021-0610**		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/884
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/885
mt6891					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/886
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	mediatek.com/product-security-bulletin/September-2021	MT68-061021/887
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/888
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/889
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-061021/890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	bulletin/September-2021	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/891
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/892
mt6893					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/894
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/895
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/897
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/898
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	H-MED-MT68-061021/899
Netgear					
gc108p					
Improper	16-Sep-21	8.3	Certain NETGEAR smart	https://kb.n	H-NET-GC10-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	etgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	061021/900
gc108pp					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to	https://kb.netgear.com/000063978/Security-	H-NET-GC10-061021/901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	
gs108t					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabiliti	H-NET-GS10-061021/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	es-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	
gs110tp					
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin	https://kb.n etgear.com/0 00063978/S ecurity-Advisory-for-Multiple-Vulnerabiliti es-on-Some-Smart-Switches-	H-NET-GS11-061021/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	
gs110tpp					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-	H-NET-GS11-061021/904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	PSV-2021-0145	
gs110tup					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	H-NET-GS11-061021/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs308t					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	H-NET-GS30-061021/906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs310tp					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	H-NET-GS31-061021/907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs710tup					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	H-NET-GS71-061021/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs716tp					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	H-NET-GS71-061021/909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs716tpp					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	H-NET-GS71-061021/910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs724tp					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	H-NET-GS72-061021/911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs724tpp					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	H-NET-GS72-061021/912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gs728tp					
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	H-NET-GS72-061021/913
gs728tpp					
Improper Authenticati	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n	https://kb.netgear.com/0	H-NET-GS72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	00063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	061021/914
gs750e					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the	https://kb.netgear.com/000063978/Security-Advisory-for-	H-NET-GS75-061021/915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	
gs752tp					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-	H-NET-GS75-061021/916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	
gs752tpp					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-	H-NET-GS75-061021/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	0140-PSV-2021-0144-PSV-2021-0145	
ms510txm					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker.	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-	H-NET-MS51-061021/918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	0145	
ms510txup					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	H-NET-MS51-061021/919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
r6020					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Sep-21	9	setup.cgi on NETGEAR R6020 1.0.0.48 devices allows an admin to execute arbitrary shell commands via shell metacharacters in the ntp_server field. **CVE ID : CVE-2021-41383**	N/A	H-NET-R602-061021/920
Phoenixcontact					
axc_f_1152					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. **CVE ID : CVE-2021-34570**	https://cert.vde.com/en/advisories/VDE-2021-029/	H-PHO-AXC_-061021/921
axc_f_2152					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. **CVE ID : CVE-2021-34570**	https://cert.vde.com/en/advisories/VDE-2021-029/	H-PHO-AXC_-061021/922
axc_f_2152_starterkit					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. **CVE ID : CVE-2021-34570**	https://cert.vde.com/en/advisories/VDE-2021-029/	H-PHO-AXC_-061021/923
axc_f_3152					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. **CVE ID : CVE-2021-34570**	https://cert.vde.com/en/advisories/VDE-2021-029/	H-PHO-AXC_-061021/924
plcnext_technology_starterkit					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. **CVE ID : CVE-2021-34570**	https://cert.vde.com/en/advisories/VDE-2021-029/	H-PHO-PLCN-061021/925
rfc_4072s					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON	https://cert.vde.com/en/advisories/VDE-2021-029/	H-PHO-RFC_-061021/926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests. **CVE ID : CVE-2021-34570**		
Qualcomm					
apq8009					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/927
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/928
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
apq8009w					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/930
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/931
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/933
apq8017					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/934
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/936
apq8037					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/937
apq8053					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature	https://www.qualcomm.com/company/product-	H-QUA-APQ8-061021/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/939
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/940
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://www.qualcomm.com/company/product-security/bull	H-QUA-APQ8-061021/941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	etins/august-2021-bulletin	
apq8064au					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/942
apq8084					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/943
apq8096au					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/944
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-061021/945
aqt1000					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AQT1-061021/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AQT1-061021/947
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AQT1-061021/948
ar6003					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AR60-061021/949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
ar7420					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AR74-061021/950
ar8031					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AR80-061021/951
ar8035					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-AR80-061021/952

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
ar9380					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AR93-061021/953
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AR93-061021/954
csr6030					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSR6-061021/955
csr8811					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSR8-061021/956
csra6620					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	H-QUA-CSRA-061021/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
csra6640					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSRA-061021/958
csrb31024					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSRB-061021/959
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://www.qualcomm.com/company/product-	H-QUA-CSRB-061021/960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	security/bulletins/august-2021-bulletin	
fsm10055					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-FSM1-061021/961
fsm10056					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-FSM1-061021/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq4018					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ4-061021/963
ipq4019					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ4-061021/964
ipq4028					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-IPQ4-061021/965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
ipq4029					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ4-061021/966
ipq5010					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ5-061021/967
ipq5018					
Use After	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-IPQ5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/968
ipq5028					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ5-061021/969
ipq6000					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	H-QUA-IPQ6-061021/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
ipq6005					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ6-061021/971
ipq6010					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ6-061021/972
ipq6018					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://www.qualcomm.com/compan	H-QUA-IPQ6-061021/973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	y/product-security/bulletins/august-2021-bulletin	
ipq6028					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ6-061021/974
ipq8064					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/976
ipq8065					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/977
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
ipq8068					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/979
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/980
ipq8069					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/982
ipq8070					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/983
ipq8070a					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-061021/984

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
ipq8071					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/985
ipq8071a					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
ipq8072					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/987
ipq8072a					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/988
ipq8074					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-IPQ8-061021/989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	-2021-bulletin	
ipq8074a					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/990
ipq8076					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq8076a					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/992
ipq8078					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/993
ipq8078a					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-IPQ8-061021/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
ipq8173					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/995
ipq8174					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-061021/996
mdm8207					
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	MDM8-061021/997
mdm8215					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-061021/998
mdm8215m					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-061021/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
mdm8615m					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-061021/1000
mdm9150					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1001
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
mdm9205					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1003
mdm9206					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1004
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM9-061021/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	etins/august-2021-bulletin	
mdm9207					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1006
mdm9215					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1007
mdm9230					
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	MDM9-061021/1008
mdm9250					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1009
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
mdm9310					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1011
mdm9330					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1012
mdm9607					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1014
mdm9615					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1015
mdm9615m					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://www.qualcomm.com/company/product-	H-QUA-MDM9-061021/1016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	security/bulletins/august-2021-bulletin	
mdm9625					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1017
mdm9626					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mdm9628					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1019
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1020
mdm9630					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
mdm9635m					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1022
mdm9640					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1023
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-MDM9-061021/1024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	-2021-bulletin	
mdm9645					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1025
mdm9650					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1026
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://www.qualcomm.	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	com/company/product-security/bulletins/august-2021-bulletin	061021/1027
mdm9655					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-061021/1028
msm8108					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
msm8208					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1030
msm8209					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1031
msm8608					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
msm8909w					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1033
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1034
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1036
msm8917					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1037
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	H-QUA-MSM8-061021/1038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1039
msm8920					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1040
msm8937					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-MSM8-061021/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	-2021-bulletin	
msm8940					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1042
msm8953					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1043
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-MSM8-061021/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1045
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1046
msm8976					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://www.qualcomm.com/compan	H-QUA-MSM8-061021/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	y/product-security/bulletins/august-2021-bulletin	
msm8976sg					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1048
msm8996au					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-061021/1050
pmp8074					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-PMP8-061021/1051
qca1990					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA1-061021/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qca4004					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA4-061021/1053
qca4020					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA4-061021/1054
qca4024					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-QCA4-061021/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
qca6174					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1056
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1057
qca6174a					
NULL Pointer	17-Sep-21	4.9	Null pointer dereference occurs due to improper	https://www.qualcomm.	H-QUA-QCA6-061021/1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	com/company/product-security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1059
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1060
qca6310					
NULL	17-Sep-21	4.9	Null pointer dereference	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/1061
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1062
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1063
qca6320					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1064
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1065
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6335					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1067
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1068
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
qca6390					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1070
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1071
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1073
qca6391					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1074
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1076
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1077
qca6420					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1079
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1080
qca6421					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1082
qca6426					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1083
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1085
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1086
qca6428					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	H-QUA-QCA6-061021/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qca6430					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1088
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1089
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qca6431					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1091
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1092
qca6436					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-QCA6-061021/1093

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-2021-1939**	-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1094
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1095
qca6438					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-061021/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	etins/august-2021-bulletin	
qca6564					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1097
qca6564a					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1099
qca6564au					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1100
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qca6574					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1102
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1103
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qca6574a					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1105
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1106
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qca6574au					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1108
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1109
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qca6584					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1111
qca6584au					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1112
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://www.qualcomm.com/company/product-	H-QUA-QCA6-061021/1113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	security/bulletins/august-2021-bulletin	
qca6595					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1114
qca6595au					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1115
Use After	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/1116
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1117
qca6694					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1119
qca6694au					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1120
qca6696					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1122
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-061021/1123
qca7500					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-QCA7-061021/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
qca7520					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA7-061021/1125
qca7550					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA7-061021/1126
qca8072					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA8-061021/1127
qca8075					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA8-061021/1128
qca8081					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA8-061021/1129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qca8337					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA8-061021/1130
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA8-061021/1131
qca9367					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-061021/1132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	etins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1133
qca9377					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1134
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCA9-061021/1135

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1136
qca9379					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1137
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://www.qualcomm.com/compan	H-QUA-QCA9-061021/1138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	y/product-security/bulletins/august-2021-bulletin	
qca9531					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1139
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1140
qca9558					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1141
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1142
qca9561					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1144
qca9563					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1145
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
qca9880					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1147
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1148
qca9882					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1150
qca9886					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1151
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qca9887					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1153
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1154
qca9888					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QCA9-061021/1155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1156
qca9889					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1157
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCA9-061021/1158

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
qca9896					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1159
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1160
qca9898					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1161
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1162
qca9980					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1164
qca9982					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1165
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
qca9984					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1167
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1168
qca9985					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qca9986					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1170
qca9987					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1171
qca9988					
Use After	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-QCA9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/1172
qca9990					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1173
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
qca9992					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1175
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1176
qca9994					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1947**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-061021/1178
qcm2290					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM2-061021/1179
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	H-QUA-QCM2-061021/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qcm4290					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM4-061021/1181
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM4-061021/1182
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM4-061021/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qcm6125					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM6-061021/1184
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM6-061021/1185
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-QCM6-061021/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	bulletin	
qcn3018					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN3-061021/1187
qcn5021					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-061021/1188
qcn5022					
Use After	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-QCN5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/1189
qcn5024					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-061021/1190
qcn5052					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	H-QUA-QCN5-061021/1191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qcn5054					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-061021/1192
qcn5064					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-061021/1193
qcn5121					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://www.qualcomm.com/compan	H-QUA-QCN5-061021/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	y/product-security/bulletins/august-2021-bulletin	
qcn5122					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-061021/1195
qcn5124					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-061021/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
qcn5152					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-061021/1197
qcn5154					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-061021/1198
qcn5164					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN5-061021/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	etins/august-2021-bulletin	
qcn5500					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-061021/1200
qcn5502					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-061021/1201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcn5550					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-061021/1202
qcn6023					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN6-061021/1203
qcn6024					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-QCN6-061021/1204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
qcn6122					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN6-061021/1205
qcn9000					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN9-061021/1206
qcn9012					
Use After	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-QCN9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/1207
qcn9022					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN9-061021/1208
qcn9024					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	H-QUA-QCN9-061021/1209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qcn9070					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN9-061021/1210
qcn9072					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN9-061021/1211
qcn9074					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://www.qualcomm.com/compan	H-QUA-QCN9-061021/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	y/product-security/bulletins/august-2021-bulletin	
qcn9100					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN9-061021/1213
qcs2290					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS2-061021/1214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS2-061021/1215
qcs405					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-061021/1216
qcs410					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-061021/1217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-061021/1218
qcs4290					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-061021/1219
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-061021/1220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-061021/1221
qcs603					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-061021/1222
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-QCS6-061021/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-061021/1224
qcs605					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-061021/1225
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-QCS6-061021/1226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-061021/1227
qcs610					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-061021/1228
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://www.qualcomm.com/compan	H-QUA-QCS6-061021/1229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	y/product-security/bulletins/august-2021-bulletin	
qcs6125					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-061021/1230
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-061021/1231
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://www.qualcomm.	H-QUA-QCS6-061021/1232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	com/company/product-security/bulletins/august-2021-bulletin	
qcx315					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCX3-061021/1233
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCX3-061021/1234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qet4101					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QET4-061021/1235
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QET4-061021/1236
qrb5165					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QRB5-061021/1237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QRB5-061021/1238
qsm8250					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QSM8-061021/1239
qsw8573					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QSW8-061021/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QSW8-061021/1241
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QSW8-061021/1242
qualcomm215					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QUAL-061021/1243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QUAL-061021/1244
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QUAL-061021/1245
sa415m					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA41-061021/1246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA41-061021/1247
sa515m					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA51-061021/1248
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA51-061021/1249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sa6145p					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-061021/1250
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-061021/1251
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-SA61-061021/1252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	bulletin	
sa6150p					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-061021/1253
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-061021/1254
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SA61-061021/1255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	-2021-bulletin	
sa6155					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-061021/1256
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-061021/1257
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA61-061021/1258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	etins/august-2021-bulletin	
sa6155p					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-061021/1259
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-061021/1260
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://www.qualcomm.com/company/product-	H-QUA-SA61-061021/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	security/bulletins/august-2021-bulletin	
sa8145p					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1262
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1263
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://www.qualcomm.com/compan	H-QUA-SA81-061021/1264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	y/product-security/bulletins/august-2021-bulletin	
sa8150p					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1265
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1266
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://www.qualcomm.	H-QUA-SA81-061021/1267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	com/company/product-security/bulletins/august-2021-bulletin	
sa8155					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1268
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1269
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	H-QUA-SA81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/1270
sa8155p					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1271
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1273
sa8195p					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1274
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-061021/1276
sc8180x\\+sdx55					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SC81-061021/1277
sd205					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD20-061021/1278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD20-061021/1279
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD20-061021/1280
sd210					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD21-061021/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD21-061021/1282
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD21-061021/1283
sd429					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD42-061021/1284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD42-061021/1285
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD42-061021/1286
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD42-061021/1287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sd439					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD43-061021/1288
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD43-061021/1289
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD43-061021/1290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sd450					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD45-061021/1291
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD45-061021/1292
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-SD45-061021/1293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	bulletin	
sd460					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD46-061021/1294
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD46-061021/1295
sd480					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature	https://www.qualcomm.com/company/product-	H-QUA-SD48-061021/1296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD48-061021/1297
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD48-061021/1298
sd632					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the	https://www.qualcomm.com/compan	H-QUA-SD63-061021/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	y/product-security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD63-061021/1300
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD63-061021/1301
sd660					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver	https://www.qualcomm.	H-QUA-SD66-061021/1302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	com/company/product-security/bulletins/august-2021-bulletin	
sd662					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-061021/1303
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-061021/1304
sd665					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-061021/1305
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-061021/1306
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-061021/1307
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	H-QUA-SD66-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/1308
sd670					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-061021/1309
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-061021/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-061021/1311
sd675					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-061021/1312
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-061021/1313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-061021/1314
sd678					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-061021/1315
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-061021/1316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-061021/1317
sd690_5g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD69-061021/1318
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD69-061021/1319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD69-061021/1320
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD69-061021/1321
sd712					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD71-061021/1322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sd720g					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD72-061021/1323
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD72-061021/1324
sd730					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SD73-061021/1325

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-2021-1939**	-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD73-061021/1326
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD73-061021/1327
sd750g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD75-061021/1328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	etins/august-2021-bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD75-061021/1329
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD75-061021/1330
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SD75-061021/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	-2021-bulletin	
sd765					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-061021/1332
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-061021/1333
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-SD76-061021/1334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-061021/1335
sd765g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-061021/1336
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SD76-061021/1337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-061021/1338
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-061021/1339
sd768g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD76-061021/1340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	etins/august-2021-bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-061021/1341
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-061021/1342
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SD76-061021/1343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	-2021-bulletin	
sd778g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD77-061021/1344
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD77-061021/1345
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD77-061021/1346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	etins/august-2021-bulletin	
sd780g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD78-061021/1347
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD78-061021/1348
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://www.qualcomm.com/company/product-	H-QUA-SD78-061021/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	security/bulletins/august-2021-bulletin	
sd820					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD82-061021/1350
sd821					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD82-061021/1351
sd835					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD83-061021/1352
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD83-061021/1353
sd845					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD84-061021/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD84-061021/1355
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD84-061021/1356
sd850					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-061021/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sd855					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-061021/1358
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-061021/1359
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-061021/1360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-061021/1361
sd865_5g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD86-061021/1362
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD86-061021/1363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1947**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD86-061021/1364
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD86-061021/1365
sd870					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD87-061021/1366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD87-061021/1367
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD87-061021/1368
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD87-061021/1369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sd888					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD88-061021/1370
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD88-061021/1371
sd888_5g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-SD88-061021/1372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD88-061021/1373
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD88-061021/1374
sda429w					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SDA4-061021/1375

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-2021-1939**	-2021-bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDA4-061021/1376
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDA4-061021/1377
sdm429w					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-SDM4-061021/1378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM4-061021/1379
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM4-061021/1380
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM4-061021/1381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sdm630					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM6-061021/1382
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM6-061021/1383
sdm830					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature	https://www.qualcomm.com/company/product-	H-QUA-SDM8-061021/1384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM8-061021/1385
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM8-061021/1386
sdw2500					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SDW2-061021/1387

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDW2-061021/1388
sdx12					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX1-061021/1389
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	H-QUA-SDX1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/1390
sdx20					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-061021/1391
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-061021/1392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
sdx20m					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-061021/1393
sdx24					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-061021/1394
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	H-QUA-SDX2-061021/1395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-061021/1396
sdx50m					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-061021/1397
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-SDX5-061021/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	bulletin	
sdx55					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-061021/1399
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-061021/1400
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-061021/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-061021/1402
sdx55m					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-061021/1403
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-SDX5-061021/1404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-061021/1405
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-061021/1406
sdxr1					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SDXR-061021/1407

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-2021-1939**	-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDXR-061021/1408
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDXR-061021/1409
sdxr2_5g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDXR-061021/1410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	etins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDXR-061021/1411
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDXR-061021/1412
sd_455					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SD_4-061021/1413

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_4-061021/1414
sd_636					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_6-061021/1415
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	H-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/1416
sd_675					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_6-061021/1417
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_6-061021/1418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_6-061021/1419
sd_8c					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_8-061021/1420
sd_8cx					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_8-061021/1421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sm4125					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM41-061021/1422
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM41-061021/1423
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM41-061021/1424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
sm6250					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62-061021/1425
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62-061021/1426
sm6250p					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-SM62-061021/1427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62-061021/1428
sm7250					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM72-061021/1429
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	H-QUA-SM72-061021/1430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM72-061021/1431
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM72-061021/1432
sm7325					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM73-061021/1433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	etins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM73-061021/1434
wcd9306					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1435
wcd9326					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver	https://www.qualcomm.	H-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	com/company/product-security/bulletins/august-2021-bulletin	061021/1436
wcd9330					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1437
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1438
wcd9335					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1439
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1440
wcd9340					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1441
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver	https://www.qualcomm.	H-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	com/company/product-security/bulletins/august-2021-bulletin	061021/1442
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1443
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1444
wcd9341					
Use After	17-Sep-21	7.2	Use-after-free vulnerability in	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	WCD9-061021/1445
wcd9360					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1446
wcd9370					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1448
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1449
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wcd9371					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1451
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1452
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
wcd9375					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1454
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1455
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1457
wcd9380					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1458
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1460
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1461
wcd9385					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1463
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1464
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-061021/1465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
wcn3610					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1466
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1467
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1469
wcn3615					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1470
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1472
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1473
wcn3620					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1475
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1476
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
wcn3660					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1478
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1479
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30261**		
wcn3660b					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1481
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1482
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1484
wcn3680					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1485
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1487
wcn3680b					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1488
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1947**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1490
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1491
wcn3910					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1493
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1494
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
wcn3950					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1496
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1497
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1499
wcn3980					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1500
wcn3988					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1502
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1503
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
wcn3990					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1505
wcn3991					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1506
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1508
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1509
wcn3998					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	H-QUA-WCN3-061021/1510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1511
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1512
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
wcn3999					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-061021/1514
wcn6740					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1515
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN6-061021/1516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	etins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1517
wcn6750					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1518
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-WCN6-061021/1519

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1520
wcn6850					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1521
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid	https://www.qualcomm.com/compan	H-QUA-WCN6-061021/1522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	y/product-security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1523
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1524
wcn6851					
NULL Pointer	17-Sep-21	4.9	Null pointer dereference occurs due to improper	https://www.qualcomm.	H-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	com/company/product-security/bulletins/august-2021-bulletin	061021/1525
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1526
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1527
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://www.qualcomm.com/compan	H-QUA-WCN6-061021/1528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	y/product-security/bulletins/august-2021-bulletin	
wcn6855					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1529
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1530
wcn6856					
NULL	17-Sep-21	4.9	Null pointer dereference	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	WCN6-061021/1531
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1532
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-061021/1533
whs9410					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WHS9-061021/1534
wsa8810					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1535
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1536
Use After	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	WSA8-061021/1537
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1538
wsa8815					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1540
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1541
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wsa8830					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1543
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1544
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1546
wsa8835					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1547
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1548
Use After	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	WSA8-061021/1549
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-061021/1550
Zyxel					
zywall_vpn2s					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Sep-21	5	A directory traversal vulnerability in the web server of the Zyxel VPN2S firmware version 1.12 could allow a remote attacker to gain access to sensitive information. **CVE ID : CVE-2021-35027**	https://www.zyxel.com/support/Zyxel_security_advisory_for_directory_traversal_and_command_injection_vulnerabilities_of_VPN2S_Firewall	H-ZYX-ZYWA-061021/1551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.shtml	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Sep-21	7.2	A command injection vulnerability in the CGI program of the Zyxel VPN2S firmware version 1.12 could allow an authenticated, local user to execute arbitrary OS commands. **CVE ID : CVE-2021-35028**	https://www.zyxel.com/support/Zyxel_security_advisory_for_directory_traversal_and_command_injection_vulnerabilities_of_VPN2S_Firewall.shtml	H-ZYX-ZYWA-061021/1552
Operating System					
Apple					
macos					
Insertion of Sensitive Information into Log File	24-Sep-21	3.6	Tor Browser through 10.5.6 and 11.x through 11.0a4 allows a correlation attack that can compromise the privacy of visits to v2 onion addresses. Exact timestamps of these onion-service visits are logged locally, and an attacker might be able to compare them to timestamp data collected by the destination server (or collected by a rogue site within the Tor network). **CVE ID : CVE-2021-39246**	https://gitlab.torproject.org/tpo/core/tor/-/commit/80c404c4b79f3bcba3fc4585d4c62a62a04f3ed9, https://gitlab.torproject.org/tpo/core/tor/-/merge_requests/434	O-APP-MACO-061021/1553
Out-of-bounds Read	29-Sep-21	6.8	Adobe InDesign versions 16.3 (and earlier), and 16.3.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	https://helpx.adobe.com/security/products/indesign/apsb21-73.html	O-APP-MACO-061021/1554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious TIF file. **CVE ID : CVE-2021-39821**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Sep-21	9.3	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary command execution vulnerability. An authenticated attacker could leverage this vulnerability to execute arbitrary commands. User interaction is required to abuse this vulnerability in that a user must open a maliciously crafted .epub file. **CVE ID : CVE-2021-39826**	https://helpx.adobe.com/security/products/Digital-Editions/apsb21-80.html	O-APP-MACO-061021/1555
Creation of Temporary File in Directory with Insecure Permissions	27-Sep-21	6.8	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary file write vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to write an arbitrary file to the system. User interaction is required before product installation to abuse this vulnerability. **CVE ID : CVE-2021-39827**	https://helpx.adobe.com/security/products/Digital-Editions/apsb21-80.html	O-APP-MACO-061021/1556
Creation of Temporary File in Directory with Insecure Permissions	27-Sep-21	6.8	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by a privilege escalation vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to escalate privileges. User	https://helpx.adobe.com/security/products/Digital-Editions/apsb21-80.html	O-APP-MACO-061021/1557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is required before product installation to abuse this vulnerability. **CVE ID : CVE-2021-39828**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Sep-21	9.3	Adobe Photoshop versions 21.2.11 (and earlier) and 22.5 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-40709**	https://helpx.adobe.com/security/products/photoshop/apsb21-84.html	O-APP-MACO-061021/1558
Improper Input Validation	29-Sep-21	4.6	Adobe Creative Cloud Desktop Application for macOS version 5.3 (and earlier) is affected by a privilege escalation vulnerability that could allow a normal user to delete the OOBE directory and get permissions of any directory under the administrator authority. **CVE ID : CVE-2021-28547**	https://helpx.adobe.com/security/products/creative-cloud/apsb21-18.html	O-APP-MACO-061021/1559
Cisco					
1100-8p_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a	https://tools.cisco.com/security/center/content/Cis	O-CIS-1100-061021/1560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	coSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	
1120_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-1120-061021/1561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1419		
1160_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-1160-061021/1562
aironet_1542d_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_1542i_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1564
aironet_1562d_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-	O-CIS-AIRO-061021/1565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	LLjsGxv	
aironet_1562e_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1566
aironet_1562i_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1567
aironet_1815i_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_1815m_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1569
aironet_1815t_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_1815w_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1571
aironet_1830e_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points	https://tools.cisco.com/security/center	O-CIS-AIRO-061021/1572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	
aironet_1830i_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_1840i_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1574
aironet_1850e_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_1850i_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1576
aironet_2800e_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-AIRO-061021/1577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	sa-cisco-ap-LLjsGxv	
aironet_2800i_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
aironet_3800e_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1579
aironet_3800i_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
aironet_3800p_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1581
aironet_4800_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-AIRO-061021/1582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_9105axi_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1583
catalyst_9105axw_firmware					
Improper Privilege	23-Sep-21	7.2	A vulnerability in the SSH management feature of	https://tools.cisco.com/se	O-CIS-CATA-061021/1584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	
catalyst_9115axe_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_9115axi_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1586
catalyst_9117_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_9120axe_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1588
catalyst_9120axi_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to	https://tools.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-CATA-061021/1589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	visory/cisco-sa-cisco-ap-LLjsGxv	
catalyst_9120axp_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
catalyst_9124axd_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1591
catalyst_9124axi_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_9130axe_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1593
catalyst_9130axi_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_9800_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1595
catalyst_iw6300_ac_firmware					
Improper Privilege	23-Sep-21	7.2	A vulnerability in the SSH management feature of	https://tools.cisco.com/se	O-CIS-CATA-061021/1596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	
catalyst_iw6300_dcw_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
catalyst_iw6300_dc_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-CATA-061021/1598
esw-6300_firmware					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-ap-LLjsGxv	O-CIS-ESW--061021/1599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user. **CVE ID : CVE-2021-1419**		
ios_xe					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device. **CVE ID : CVE-2021-34723**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxesdwan-arbfileov-MVOF3ZZn	O-CIS-IOS_-061021/1600
vedge_1000_firmware					
Generation of Error Message Containing Sensitive	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This	https://tools.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-VEDG-061021/1601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	visory/cisco-sa-sd-wan-Fhqh8pKX	
vedge_100b_firmware					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	O-CIS-VEDG-061021/1602
vedge_100m_firmware					
Generation of Error Message Containing	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access	https://tools.cisco.com/security/center/content/Cis	O-CIS-VEDG-061021/1603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	coSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	
vedge_100wm_firmware					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	O-CIS-VEDG-061021/1604
vedge_100_firmware					
Generation of Error Message	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated,	https://tools.cisco.com/security/center	O-CIS-VEDG-061021/1605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Containing Sensitive Information			local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	
vedge_2000_firmware					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	O-CIS-VEDG-061021/1606
vedge_5000_firmware					
Generation of Error	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software	https://tools.cisco.com/se	O-CIS-VEDG-061021/1607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Message Containing Sensitive Information			could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	
vedge_cloud_firmware					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	O-CIS-VEDG-061021/1608
vsmart_controller_firmware					
Generation	23-Sep-21	2.1	A vulnerability in the CLI of	https://tools.	O-CIS-VSMA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Error Message Containing Sensitive Information			Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2021-1546**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX	061021/1609
D-link					
dcs-5000l_firmware					
Improper Authentication	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** DCS-5000L v1.05 and DCS-932L v2.17 and older are affecged by Incorrect Acess Control. The use of the basic authentication for the devices command interface allows attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-41503**	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10247	O-D-L-DCS--061021/1610
Improper Privilege	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** An Elevated	https://www.dlink.com/	O-D-L-DCS--061021/1611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Privileges issue exists in D-Link DCS-5000L v1.05 and DCS-932L v2.17 and older. The use of the digest-authentication for the devices command interface may allow further attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-41504**	en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10247	
dcs-932l_firmware					
Improper Authentication	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** DCS-5000L v1.05 and DCS-932L v2.17 and older are affecged by Incorrect Acess Control. The use of the basic authentication for the devices command interface allows attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-41503**	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10247	O-D-L-DCS--061021/1612
Improper Privilege Management	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** An Elevated Privileges issue exists in D-Link DCS-5000L v1.05 and DCS-932L v2.17 and older.	https://www.dlink.com/en/security-bulletin/, https://supp	O-D-L-DCS--061021/1613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The use of the digest-authentication for the devices command interface may allow further attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-41504**	ortannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10247	
Debian					
debian_linux					
Exposure of Sensitive Information to an Unauthorized Actor	19-Sep-21	5	All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfo from a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element. **CVE ID : CVE-2021-40690**	https://lists.apache.org/thread.html/r8848751b6a5dd78cc9e99d627e74fecfaffdfa1bb615dce827aad633%40%3Cdev.santuario.apache.org%3E, https://lists.apache.org/thread.html/rbdac116aef912b563da54f4c152222c0754e32fb2f785519ac5e059f@%3Ccommits.tomee.apache.org%3E	O-DEB-DEBI-061021/1614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	19-Sep-21	7.2	loop_rw_iter in fs/io_uring.c in the Linux kernel 5.10 through 5.14.6 allows local users to gain privileges by using IORING_OP_PROVIDE_BUFFERS to trigger a free of a kernel buffer, as demonstrated by using /proc/<pid>/maps for exploitation. **CVE ID : CVE-2021-41073**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=16c8d2df7ec0eed31b7d3b61cb13206a7fb930cc	O-DEB-DEBI-061021/1615
Improper Input Validation	16-Sep-21	4.3	Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service. **CVE ID : CVE-2021-41079**	https://lists.apache.org/thread.html/rccdef0349fdf4fb73a4e4403095446d7fe6264e0a58e2df5c6799434%40%3Cannounce.tomcat.apache.org%3E	O-DEB-DEBI-061021/1616
Dlink					
dir-3040_firmware					
Use of Hard-coded Credentials	23-Sep-21	7.5	An information disclosure vulnerability exists in the WiFi Smart Mesh functionality of D-LINK DIR-3040 1.13B03. A specially-crafted network request can lead to command execution. An attacker can connect to the MQTT service to trigger this vulnerability. **CVE ID : CVE-2021-21913**	N/A	O-DLI-DIR--061021/1617
dir-605l_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	24-Sep-21	5	An informtion disclosure issue exists in D-LINK-DIR-605 B2 Firmware Version : 2.01MT. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page **CVE ID : CVE-2021-40655**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--061021/1618
dir-615_firmware					
Insufficiently Protected Credentials	24-Sep-21	4	An information disclosure issue exist in D-LINK-DIR-615 B2 2.01mt. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page **CVE ID : CVE-2021-40654**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--061021/1619
Fedoraproject					
fedora					
Use After Free	17-Sep-21	3.3	Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing `externref`s from the host to guest Wasm content. To trigger the bug, you have to explicitly pass multiple `externref`s from the host to a Wasm instance at the same time, either by passing multiple `externref`s as arguments from host code to a Wasm function, or returning multiple `externref`s to Wasm from a multi-value return function	https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-v4cp-h94r-m7xf	O-FED-FEDO-061021/1620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			defined in the host. If you do not have host code that matches one of these shapes, then you are not impacted. If Wasmtime's `VMExternRefActivationsTable` became filled to capacity after passing the first `externref` in, then passing in the second `externref` could trigger a garbage collection. However the first `externref` is not rooted until we pass control to Wasm, and therefore could be reclaimed by the collector if nothing else was holding a reference to it or otherwise keeping it alive. Then, when control was passed to Wasm after the garbage collection, Wasm could use the first `externref`, which at this point has already been freed. We have reason to believe that the effective impact of this bug is relatively small because usage of `externref` is currently quite rare. The bug has been fixed, and users should upgrade to Wasmtime 0.30.0. If you cannot upgrade Wasmtime yet, you can avoid the bug by disabling reference types support in Wasmtime by passing `false` to `wasmtime::Config::wasm_reference_types`. **CVE ID : CVE-2021-39216**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	17-Sep-21	3.3	Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.26.0 and before version 0.30.0 is affected by a memory unsoundness vulnerability. There was an invalid free and out-of-bounds read and write bug when running Wasm that uses `externref`s in Wasmtime. To trigger this bug, Wasmtime needs to be running Wasm that uses `externref`s, the host creates non-null `externrefs`, Wasmtime performs a garbage collection (GC), and there has to be a Wasm frame on the stack that is at a GC safepoint where there are no live references at this safepoint, and there is a safepoint with live references earlier in this frame's function. Under this scenario, Wasmtime would incorrectly use the GC stack map for the safepoint from earlier in the function instead of the empty safepoint. This would result in Wasmtime treating arbitrary stack slots as `externref`s that needed to be rooted for GC. At the *next* GC, it would be determined that nothing was referencing these bogus `externref`s (because nothing could ever reference them, because they are not really `externref`s)	https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-4873-36h9-wv49, https://github.com/bytecodealliance/wasmtime/commit/398a73f0dd862dbe703212ebae8e34036a18c11c	O-FED-FEDO-061021/1621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and then Wasmtime would deallocate them and run `<ExternRef as Drop>::drop` on them. This results in a free of memory that is not necessarily on the heap (and shouldn't be freed at this moment even if it was), as well as potential out-of-bounds reads and writes. Even though support for `externref`s (via the reference types proposal) is enabled by default, unless you are creating non-null `externref`s in your host code or explicitly triggering GCs, you cannot be affected by this bug. We have reason to believe that the effective impact of this bug is relatively small because usage of `externref` is currently quite rare. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime at this time, you can avoid this bug by disabling the reference types proposal by passing `false` to `wasmtime::Config::wasm_reference_types`. **CVE ID : CVE-2021-39218**		
Access of Resource Using Incompatible Type ('Type Confusion')	17-Sep-21	3.3	Wasmtime is an open source runtime for WebAssembly & WASI. Wasmtime before version 0.30.0 is affected by a type confusion vulnerability. As a Rust library the	https://github.com/bytecodealliance/wasmtime/commit/b39f087414f27ae	O-FED-FEDO-061021/1622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			`wasmtime` crate clearly marks which functions are safe and which are `unsafe`, guaranteeing that if consumers never use `unsafe` then it should not be possible to have memory unsafety issues in their embeddings of Wasmtime. An issue was discovered in the safe API of `Linker::func_*` APIs. These APIs were previously not sound when one `Engine` was used to create the `Linker` and then a different `Engine` was used to create a `Store` and then the `Linker` was used to instantiate a module into that `Store`. Cross-`Engine` usage of functions is not supported in Wasmtime and this can result in type confusion of function pointers, resulting in being able to safely call a function with the wrong type. Triggering this bug requires using at least two `Engine` values in an embedding and then additionally using two different values with a `Linker` (one at the creation time of the `Linker` and another when instantiating a module with the `Linker`). It's expected that usage of more-than-one `Engine` in an embedding is relatively rare since an `Engine` is intended to be a globally shared resource, so the expectation	40c44449ed5d1154e03449bff, https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-q879-9g95-56mx	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is that the impact of this issue is relatively small. The fix implemented is to change this behavior to `panic!()` in Rust instead of silently allowing it. Using different `Engine` instances with a `Linker` is a programmer bug that `wasmtime` catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`. **CVE ID : CVE-2021-39219**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-21	7.5	ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier. **CVE ID : CVE-2021-39275**	https://httpd.apache.org/security/vulnerabilities_24.html, https://lists.apache.org/thread.html/r82c077663f9759c7df5a6656f925b3ee4	O-FED-FEDO-061021/1623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				f55fcd33c889ba7cd687029@%3Cusers.httpd.apache.org%3E	
Server-Side Request Forgery (SSRF)	16-Sep-21	7.5	A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier. **CVE ID : CVE-2021-40438**	https://httpd.apache.org/security/vulnerabilities_24.html, https://lists.apache.org/thread.html/r82c077663f9759c7df5a6656f925b3ee4f55fcd33c889ba7cd687029@%3Cusers.httpd.apache.org%3E	O-FED-FEDO-061021/1624
Uncontrolled Resource Consumption	20-Sep-21	5	Flask-RESTX (pypi package flask-restx) is a community driven fork of Flask-RESTPlus. Flask-RESTX before version 0.5.1 is vulnerable to ReDoS (Regular Expression Denial of Service) in email_regex. This is fixed in version 0.5.1. **CVE ID : CVE-2021-32838**	https://github.com/python-restx/flask-restx/issues/372, https://github.com/python-restx/flask-restx/commit/bab31e085f355dd73858fd3715f7ed71849656da, https://github.com/advisories/GHSA-3q6g-vf58-	O-FED-FEDO-061021/1625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				7m4g	
NULL Pointer Dereference	16-Sep-21	5	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier. **CVE ID : CVE-2021-34798**	http://httpd.apache.org/security/vulnerabilities_24.html, https://lists.apache.org/thread.html/r82c077663f9759c7df5a6656f925b3ee4f55fcd33c889ba7cd687029@%3Cusers.httpd.apache.org%3E	O-FED-FEDO-061021/1626
Out-of-bounds Read	16-Sep-21	5	A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive). **CVE ID : CVE-2021-36160**	http://httpd.apache.org/security/vulnerabilities_24.html, https://lists.apache.org/thread.html/ree7519d71415ecdd170ff1889cab552d71758d2ba2904a17ded21a70@%3Ccvs.httpd.apache.org%3E	O-FED-FEDO-061021/1627
Google					
android					
Improper Restriction of Operations	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead	https://corp.mediatek.com/product-security-	O-GOO-ANDR-061021/1628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071. **CVE ID : CVE-2021-0422**	bulletin/September-2021	
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714. **CVE ID : CVE-2021-0423**	https://corp.mediatek.com/product-security-bulletin/September-2021	O-GOO-ANDR-061021/1629
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. **CVE ID : CVE-2021-0424**	https://corp.mediatek.com/product-security-bulletin/September-2021	O-GOO-ANDR-061021/1630
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/September-2021	O-GOO-ANDR-061021/1631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. **CVE ID : CVE-2021-0425**		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456. **CVE ID : CVE-2021-0610**	https://corp.mediatek.com/product-security-bulletin/September-2021	O-GOO-ANDR-061021/1632
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425810. **CVE ID : CVE-2021-0611**	https://corp.mediatek.com/product-security-bulletin/September-2021	O-GOO-ANDR-061021/1633
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption 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. Patch ID: ALPS05403499; Issue ID: ALPS05425834. **CVE ID : CVE-2021-0612**	https://corp.mediatek.com/product-security-bulletin/September-2021	O-GOO-ANDR-061021/1634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	27-Sep-21	4	In ccu, there is a possible out of bounds read due to incorrect error handling. This could lead to information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827145; Issue ID: ALPS05827145. **CVE ID : CVE-2021-0660**	https://corp.mediatek.com/product-security-bulletin/September-2021	O-GOO-ANDR-061021/1635
IBM					
aix					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored 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: 208405. **CVE ID : CVE-2021-38877**	https://exchange.xforce.ibmcloud.com/vulnerabilities/208405, https://www.ibm.com/support/pages/node/6491521	O-IBM-AIX-061021/1636
Allocation of Resources Without Limits or Throttling	16-Sep-21	1.9	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267. **CVE ID : CVE-2021-29763**	https://www.ibm.com/support/pages/node/6489493, https://exchange.xforce.ibmcloud.com/vulnerabilities/202267	O-IBM-AIX-061021/1637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204279. **CVE ID : CVE-2021-29810**	https://www.ibm.com/support/pages/node/6491547, https://exchange.xforce.ibmcloud.com/vulnerabilities/204279	O-IBM-AIX-061021/1638
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204330. **CVE ID : CVE-2021-29812**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204330, https://www.ibm.com/support/pages/node/6491545	O-IBM-AIX-061021/1639
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript	https://exchange.xforce.ibmcloud.com/vulnerabilities/204331, https://www.ibm.com/support/page	O-IBM-AIX-061021/1640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204331. **CVE ID : CVE-2021-29813**	s/node/6491543	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204334. **CVE ID : CVE-2021-29814**	https://www.ibm.com/support/pages/node/6491539, https://exchange.xforce.ibmcloud.com/vulnerabilities/204334	O-IBM-AIX-061021/1641
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204340.	https://www.ibm.com/support/pages/node/6491537, https://exchange.xforce.ibmcloud.com/vulnerabilities/204340	O-IBM-AIX-061021/1642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29815		
Cross-Site Request Forgery (CSRF)	23-Sep-21	4.3	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 204341. **CVE ID : CVE-2021-29816**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204341, https://www.ibm.com/support/pages/node/6491535	O-IBM-AIX-061021/1643
Exposure of Sensitive Information to an Unauthorized Actor	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470. **CVE ID : CVE-2021-29825**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204470, https://www.ibm.com/support/pages/node/6489499	O-IBM-AIX-061021/1644
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204824. **CVE ID : CVE-2021-29832**	https://www.ibm.com/support/pages/node/6491529, https://exchange.xforce.ibmcloud.com/vulnerabilities/204824	O-IBM-AIX-061021/1645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204825. **CVE ID : CVE-2021-29833**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204825, https://www.ibm.com/support/pages/node/6491527	O-IBM-AIX-061021/1646
Cleartext Storage of Sensitive Information	23-Sep-21	2.1	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI displays user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 207610. **CVE ID : CVE-2021-29904**	https://www.ibm.com/support/pages/node/6491525, https://exchange.xforce.ibmcloud.com/vulnerabilities/207610	O-IBM-AIX-061021/1647
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI 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: 207616.	https://www.ibm.com/support/pages/node/6491523, https://exchange.xforce.ibmcloud.com/vulnerabilities/207616	O-IBM-AIX-061021/1648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29905		
powervm_hypervisor					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Sep-21	4.9	IBM PowerVM Hypervisor FW860, FW930, FW940, and FW950 could allow a local user to create a specially crafted sequence of hypervisor calls from a partition that could crash the system. IBM X-Force ID: 203557. **CVE ID : CVE-2021-29795**	https://exchange.xforce.ibmcloud.com/vulnerabilities/203557, https://www.ibm.com/support/pages/node/6490877	O-IBM-POWE-061021/1649
kadenvodomery					
picoflux_air_firmware					
Observable Discrepancy	16-Sep-21	3.3	In Kaden PICOFLUX Air in all known versions an information exposure through observable discrepancy exists. This may give sensitive information (water consumption without distinct values) to third parties. **CVE ID : CVE-2021-34576**	https://www.fit.vutbr.cz/~polcak/CVE-2021-34576.en	O-KAD-PICO-061021/1650
Linux					
linux_kernel					
N/A	20-Sep-21	7.2	arch/mips/net/bpf_jit.c in the Linux kernel through 5.14.6 can generate undesirable machine code when transforming unprivileged cBPF programs, allowing execution of arbitrary code within the kernel context. This occurs because conditional branches can exceed the 128 KB limit	http://www.openwall.com/lists/oss-security/2021/09/15/5	O-LIN-LINU-061021/1651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the MIPS architecture. **CVE ID : CVE-2021-38300**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored 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: 208405. **CVE ID : CVE-2021-38877**	https://exchange.xforce.ibmcloud.com/vulnerabilities/208405, https://www.ibm.com/support/pages/node/6491521	O-LIN-LINU-061021/1652
Insertion of Sensitive Information into Log File	24-Sep-21	3.6	Tor Browser through 10.5.6 and 11.x through 11.0a4 allows a correlation attack that can compromise the privacy of visits to v2 onion addresses. Exact timestamps of these onion-service visits are logged locally, and an attacker might be able to compare them to timestamp data collected by the destination server (or collected by a rogue site within the Tor network). **CVE ID : CVE-2021-39246**	https://gitlab.torproject.org/tpo/core/tor/-/commit/80c404c4b79f3bcba3fc4585d4c62a62a04f3ed9, https://gitlab.torproject.org/tpo/core/tor/-/merge_requests/434	O-LIN-LINU-061021/1653
Improper Privilege Management	19-Sep-21	7.2	loop_rw_iter in fs/io_uring.c in the Linux kernel 5.10 through 5.14.6 allows local users to gain privileges by using IORING_OP_PROVIDE_BUFFERS to trigger a free of a kernel buffer, as demonstrated by	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=16c8d2df7ec0eed31	O-LIN-LINU-061021/1654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using /proc/<pid>/maps for exploitation. **CVE ID : CVE-2021-41073**	b7d3b61cb13206a7fb930cc	
Allocation of Resources Without Limits or Throttling	16-Sep-21	1.9	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267. **CVE ID : CVE-2021-29763**	https://www.ibm.com/support/pages/node/6489493, https://exchange.xforce.ibmcloud.com/vulnerabilities/202267	O-LIN-LINU-061021/1655
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204279. **CVE ID : CVE-2021-29810**	https://www.ibm.com/support/pages/node/6491547, https://exchange.xforce.ibmcloud.com/vulnerabilities/204279	O-LIN-LINU-061021/1656
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript	https://exchange.xforce.ibmcloud.com/vulnerabilities/204330, https://www.ibm.com/support/page	O-LIN-LINU-061021/1657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204330. **CVE ID : CVE-2021-29812**	s/node/6491545	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204331. **CVE ID : CVE-2021-29813**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204331, https://www.ibm.com/support/pages/node/6491543	O-LIN-LINU-061021/1658
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204334.	https://www.ibm.com/support/pages/node/6491539, https://exchange.xforce.ibmcloud.com/vulnerabilities/204334	O-LIN-LINU-061021/1659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29814		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204340. **CVE ID : CVE-2021-29815**	https://www.ibm.com/support/pages/node/6491537, https://exchange.xforce.ibmcloud.com/vulnerabilities/204340	O-LIN-LINU-061021/1660
Cross-Site Request Forgery (CSRF)	23-Sep-21	4.3	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 204341. **CVE ID : CVE-2021-29816**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204341, https://www.ibm.com/support/pages/node/6491535	O-LIN-LINU-061021/1661
Exposure of Sensitive Information to an Unauthorized Actor	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470. **CVE ID : CVE-2021-29825**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204470, https://www.ibm.com/support/pages/node/6489499	O-LIN-LINU-061021/1662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204824. **CVE ID : CVE-2021-29832**	https://www.ibm.com/support/pages/node/6491529, https://exchange.xforce.ibmcloud.com/vulnerabilities/204824	O-LIN-LINU-061021/1663
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204825. **CVE ID : CVE-2021-29833**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204825, https://www.ibm.com/support/pages/node/6491527	O-LIN-LINU-061021/1664
Cleartext Storage of Sensitive Information	23-Sep-21	2.1	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI displays user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 207610.	https://www.ibm.com/support/pages/node/6491525, https://exchange.xforce.ibmcloud.com	O-LIN-LINU-061021/1665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29904	/vulnerabilities/207610	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI 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: 207616. **CVE ID : CVE-2021-29905**	https://www.ibm.com/support/pages/node/6491523, https://exchange.xforce.ibmcloud.com/vulnerabilities/207616	O-LIN-LINU-061021/1666
Microsoft					
windows					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored 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: 208405. **CVE ID : CVE-2021-38877**	https://exchange.xforce.ibmcloud.com/vulnerabilities/208405, https://www.ibm.com/support/pages/node/6491521	O-MIC-WIND-061021/1667
Insertion of Sensitive Information into Log File	24-Sep-21	3.6	Tor Browser through 10.5.6 and 11.x through 11.0a4 allows a correlation attack that can compromise the privacy of visits to v2 onion addresses. Exact timestamps	https://gitlab.torproject.org/tpo/core/tor/-/commit/80c404c4b79f3	O-MIC-WIND-061021/1668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of these onion-service visits are logged locally, and an attacker might be able to compare them to timestamp data collected by the destination server (or collected by a rogue site within the Tor network). **CVE ID : CVE-2021-39246**	bcba3fc4585d4c62a62a04f3ed9, https://gitlab.torproject.org/tpo/core/tor/-/merge_requests/434	
Out-of-bounds Read	29-Sep-21	6.8	Adobe InDesign versions 16.3 (and earlier), and 16.3.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious TIF file. **CVE ID : CVE-2021-39821**	https://helpx.adobe.com/security/products/indesign/apsb21-73.html	O-MIC-WIND-061021/1669
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Sep-21	9.3	Adobe Photoshop versions 21.2.11 (and earlier) and 22.5 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-40709**	https://helpx.adobe.com/security/products/photoshop/apsb21-84.html	O-MIC-WIND-061021/1670
Improper	29-Sep-21	4.6	Adobe Creative Cloud	https://help	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Desktop Application for macOS version 5.3 (and earlier) is affected by a privilege escalation vulnerability that could allow a normal user to delete the OOBE directory and get permissions of any directory under the administrator authority. **CVE ID : CVE-2021-28547**	x.adobe.com/security/products/creative-cloud/apsb21-18.html	061021/1671
Allocation of Resources Without Limits or Throttling	16-Sep-21	1.9	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267. **CVE ID : CVE-2021-29763**	https://www.ibm.com/support/pages/node/6489493, https://exchange.xforce.ibmcloud.com/vulnerabilities/202267	O-MIC-WIND-061021/1672
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204279. **CVE ID : CVE-2021-29810**	https://www.ibm.com/support/pages/node/6491547, https://exchange.xforce.ibmcloud.com/vulnerabilities/204279	O-MIC-WIND-061021/1673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204330. **CVE ID : CVE-2021-29812**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204330, https://www.ibm.com/support/pages/node/6491545	O-MIC-WIND-061021/1674
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204331. **CVE ID : CVE-2021-29813**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204331, https://www.ibm.com/support/pages/node/6491543	O-MIC-WIND-061021/1675
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript	https://www.ibm.com/support/pages/node/6491539, https://exchange.xforce.ibmcloud.com	O-MIC-WIND-061021/1676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204334. **CVE ID : CVE-2021-29814**	/vulnerabilities/204334	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204340. **CVE ID : CVE-2021-29815**	https://www.ibm.com/support/pages/node/6491537, https://exchange.xforce.ibmcloud.com/vulnerabilities/204340	O-MIC-WIND-061021/1677
Cross-Site Request Forgery (CSRF)	23-Sep-21	4.3	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 204341. **CVE ID : CVE-2021-29816**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204341, https://www.ibm.com/support/pages/node/6491535	O-MIC-WIND-061021/1678
Exposure of Sensitive Information	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could	https://exchange.xforce.ibmcloud.com	O-MIC-WIND-061021/1679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to an Unauthorized Actor			disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470. **CVE ID : CVE-2021-29825**	/vulnerabilities/204470, https://www.ibm.com/support/pages/node/6489499	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204824. **CVE ID : CVE-2021-29832**	https://www.ibm.com/support/pages/node/6491529, https://exchange.xforce.ibmcloud.com/vulnerabilities/204824	O-MIC-WIND-061021/1680
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored 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: 204825. **CVE ID : CVE-2021-29833**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204825, https://www.ibm.com/support/pages/node/6491527	O-MIC-WIND-061021/1681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	23-Sep-21	2.1	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI displays user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 207610. **CVE ID : CVE-2021-29904**	https://www.ibm.com/support/pages/node/6491525, https://exchange.xforce.ibmcloud.com/vulnerabilities/207610	O-MIC-WIND-061021/1682
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI 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: 207616. **CVE ID : CVE-2021-29905**	https://www.ibm.com/support/pages/node/6491523, https://exchange.xforce.ibmcloud.com/vulnerabilities/207616	O-MIC-WIND-061021/1683
Uncontrolled Search Path Element	29-Sep-21	6.9	An uncontrolled search path element privilege escalation vulnerability in Trend Micro HouseCall for Home Networks version 5.3.1225 and below could allow an attacker to escalate privileges by placing a custom crafted file in a specific directory to load a malicious library. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://helpcenter.trendmicro.com/ja-jp/article/TMKA-10621, https://helpcenter.trendmicro.com/en-us/article/tmka-10626	O-MIC-WIND-061021/1684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-32466		
Netgear					
gc108pp_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	O-NET-GC10-061021/1685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gc108p_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	O-NET-GC10-061021/1686
gs108t_firmware					
Improper Authenticati	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n	https://kb.netgear.com/0	O-NET-GS10-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	00063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	061021/1687
gs110tpp_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the	https://kb.netgear.com/000063978/Security-Advisory-for-	O-NET-GS11-061021/1688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	
gs110tp_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-	O-NET-GS11-061021/1689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	
gs110tup_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-	O-NET-GS11-061021/1690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	0140-PSV-2021-0144-PSV-2021-0145	
gs308t_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker.	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-	O-NET-GS30-061021/1691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	0145	
gs310tp_firmware					
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before	https://kb.n etgear.com/0 00063978/S ecurity-Advisory-for-Multiple-Vulnerabiliti es-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	O-NET-GS31-061021/1692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs710tup_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	O-NET-GS71-061021/1693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs716tpp_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	O-NET-GS71-061021/1694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs716tp_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	O-NET-GS71-061021/1695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs724tpp_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	O-NET-GS72-061021/1696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs724tp_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	O-NET-GS72-061021/1697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**		
gs728tpp_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	O-NET-GS72-061021/1698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-41314		
gs728tp_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	O-NET-GS72-061021/1699
gs750e_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	O-NET-GS75-061021/1700
gs752tpp_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's	https://kb.netgear.com/000063978/S	O-NET-GS75-061021/1701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	ecurity-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	
gs752tp_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme -	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-	O-NET-GS75-061021/1702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	
ms510txm_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2"	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-	O-NET-MS51-061021/1703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0145	
ms510txup_firmware					
Improper Authentication	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin	https://kb.netgear.com/000063978/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Smart-Switches-PSV-2021-0140-PSV-	O-NET-MS51-061021/1704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. **CVE ID : CVE-2021-41314**	2021-0144-PSV-2021-0145	
r6020_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Sep-21	9	setup.cgi on NETGEAR R6020 1.0.0.48 devices allows an admin to execute arbitrary shell commands via shell metacharacters in the ntp_server field. **CVE ID : CVE-2021-41383**	N/A	O-NET-R602-061021/1705
opengroup					
unix					
Allocation of Resources Without Limits or	16-Sep-21	1.9	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific	https://www.ibm.com/support/pages/node/6489	O-OPE-UNIX-061021/1706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Throttling			conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267. **CVE ID : CVE-2021-29763**	493, https://exchange.xforce.ibmcloud.com/vulnerabilities/202267	
Exposure of Sensitive Information to an Unauthorized Actor	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470. **CVE ID : CVE-2021-29825**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204470, https://www.ibm.com/support/pages/node/6489499	O-OPE-UNIX-061021/1707
Oracle					
linux					
N/A	24-Sep-21	7.2	Vulnerability in Oracle Linux (component: OSwatcher). Supported versions that are affected are 7 and 8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Linux executes to compromise Oracle Linux. Successful attacks of this vulnerability can result in takeover of Oracle Linux. 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).	https://linux.oracle.com/errata/ELSA-2021-9444.html	O-ORA-LINU-061021/1708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-2464		
solaris					
Allocation of Resources Without Limits or Throttling	16-Sep-21	1.9	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267. **CVE ID : CVE-2021-29763**	https://www.ibm.com/support/pages/node/6489493, https://exchange.xforce.ibmcloud.com/vulnerabilities/202267	O-ORA-SOLA-061021/1709
Exposure of Sensitive Information to an Unauthorized Actor	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470. **CVE ID : CVE-2021-29825**	https://exchange.xforce.ibmcloud.com/vulnerabilities/204470, https://www.ibm.com/support/pages/node/6489499	O-ORA-SOLA-061021/1710
Phoenixcontact					
axc_f_1152_firmware					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. **CVE ID : CVE-2021-34570**	https://cert.vde.com/en/advisories/VDE-2021-029/	O-PHO-AXC_-061021/1711
axc_f_2152_firmware					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack	https://cert.vde.com/en/advisories/VDE-2021-	O-PHO-AXC_-061021/1712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through special crafted JSON requests. **CVE ID : CVE-2021-34570**	029/	
axc_f_2152_starterkit_firmware					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. **CVE ID : CVE-2021-34570**	https://cert.vde.com/en/advisories/VDE-2021-029/	O-PHO-AXC_-061021/1713
axc_f_3152_firmware					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. **CVE ID : CVE-2021-34570**	https://cert.vde.com/en/advisories/VDE-2021-029/	O-PHO-AXC_-061021/1714
plcnext_technology_starterkit_firmware					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. **CVE ID : CVE-2021-34570**	https://cert.vde.com/en/advisories/VDE-2021-029/	O-PHO-PLCN-061021/1715
rfc_4072s_firmware					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. **CVE ID : CVE-2021-34570**	https://cert.vde.com/en/advisories/VDE-2021-029/	O-PHO-RFC_-061021/1716
Qualcomm					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
apq8009w_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1717
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1718
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1720
apq8009_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1721
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1723
apq8017_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1724
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1726
apq8037_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1727
apq8053_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1729
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1730
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
apq8064au_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1732
apq8084_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1733
apq8096au_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-APQ8-061021/1734

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-061021/1735
aqt1000_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AQT1-061021/1736
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://www.qualcomm.com/compan	O-QUA-AQT1-061021/1737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	y/product-security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AQT1-061021/1738
ar6003_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR60-061021/1739
ar7420_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR74-061021/1740
ar8031_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR80-061021/1741
ar8035_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR80-061021/1742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
ar9380_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR93-061021/1743
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR93-061021/1744
csr6030_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://www.qualcomm.com/company/product-security/bull	O-QUA-CSR6-061021/1745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	etins/august-2021-bulletin	
csr8811_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSR8-061021/1746
csra6620_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRA-061021/1747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
csra6640_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRA-061021/1748
csrb31024_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRB-061021/1749
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRB-061021/1750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
fsm10055_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-FSM1-061021/1751
fsm10056_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-FSM1-061021/1752
ipq4018_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://www.qualcomm.com/compan	O-QUA-IPQ4-061021/1753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	y/product-security/bulletins/august-2021-bulletin	
ipq4019_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ4-061021/1754
ipq4028_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ4-061021/1755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
ipq4029_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ4-061021/1756
ipq5010_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ5-061021/1757
ipq5018_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ5-061021/1758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	etins/august-2021-bulletin	
ipq5028_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ5-061021/1759
ipq6000_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ6-061021/1760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq6005_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ6-061021/1761
ipq6010_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ6-061021/1762
ipq6018_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	O-QUA-IPQ6-061021/1763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
ipq6028_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ6-061021/1764
ipq8064_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1765
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-061021/1766

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
ipq8065_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1767
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1768
ipq8068_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1769
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1770
ipq8069_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1772
ipq8070a_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1773
ipq8070_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
ipq8071a_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1775
ipq8071_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1776
ipq8072a_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P	https://www.qualcomm.	O-QUA-IPQ8-061021/1777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	com/company/product-security/bulletins/august-2021-bulletin	
ipq8072_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1778
ipq8074a_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1976**		
ipq8074_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1780
ipq8076a_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1781
ipq8076_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-061021/1782

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
ipq8078a_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1783
ipq8078_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
ipq8173_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1785
ipq8174_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-061021/1786
mdm8207_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-MDM8-061021/1787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	-2021-bulletin	
mdm8215m_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-061021/1788
mdm8215_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-061021/1789
mdm8615m_firmware					
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://www.qualcomm.	O-QUA-MDM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	com/company/product-security/bulletins/august-2021-bulletin	061021/1790
mdm9150_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1791
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mdm9205_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1793
mdm9206_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1794
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
mdm9207_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1796
mdm9215_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1797
mdm9230_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-MDM9-061021/1798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	-2021-bulletin	
mdm9250_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1799
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1800
mdm9310_firmware					
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://www.qualcomm.	O-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	com/company/product-security/bulletins/august-2021-bulletin	061021/1801
mdm9330_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1802
mdm9607_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1804
mdm9615m_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1805
mdm9615_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
mdm9625_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1807
mdm9626_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1808
mdm9628_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-MDM9-061021/1809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	etins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1810
mdm9630_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1811
mdm9635m_firmware					
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	MDM9-061021/1812
mdm9640_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1813
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
mdm9645_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1815
mdm9650_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1816
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
mdm9655_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-061021/1818
msm8108_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1819
msm8208_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://www.qualcomm.com/company/product-security/bull	O-QUA-MSM8-061021/1820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	etins/august-2021-bulletin	
msm8209_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1821
msm8608_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1822
msm8909w_firmware					
NULL	17-Sep-21	4.9	Null pointer dereference	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	MSM8-061021/1823
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1824
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1825
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://www.qualcomm.	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	com/company/product-security/bulletins/august-2021-bulletin	061021/1826
msm8917_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1827
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1828
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	MSM8-061021/1829
msm8920_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1830
msm8937_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
msm8940_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1832
msm8953_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1833
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1947**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1835
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1836
msm8976sg_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
msm8976_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1838
msm8996au_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-061021/1839
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://www.qualcomm.com/company/product-security/bull	O-QUA-MSM8-061021/1840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	etins/august-2021-bulletin	
pmp8074_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-PMP8-061021/1841
qca1990_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA1-061021/1842
qca4004_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA4-061021/1843
qca4020_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA4-061021/1844
qca4024_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA4-061021/1845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
qca6174a_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1846
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1847
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qca6174_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1849
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1850
qca6310_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-QCA6-061021/1851

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-2021-1939**	-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1852
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1853
qca6320_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-061021/1854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	etins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1855
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1856
qca6335_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature	https://www.qualcomm.com/company/product-	O-QUA-QCA6-061021/1857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1858
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1859
qca6390_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the	https://www.qualcomm.com/compan	O-QUA-QCA6-061021/1860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	y/product-security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1861
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1862
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://www.qualcomm.com/company/product-	O-QUA-QCA6-061021/1863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	security/bulletins/august-2021-bulletin	
qca6391_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1864
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1865
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-061021/1866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	etins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1867
qca6420_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1868
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCA6-061021/1869

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1870
qca6421_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1871
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://www.qualcomm.com/compan	O-QUA-QCA6-061021/1872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	y/product-security/bulletins/august-2021-bulletin	
qca6426_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1873
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1874
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCA6-061021/1875

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1876
qca6428_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1877
qca6430_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1878
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1879
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6431_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1881
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1882
qca6436_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1884
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1885
qca6438_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qca6564au_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1887
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1888
qca6564a_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-QCA6-061021/1889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1890
qca6564_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1891
qca6574au_firmware					
NULL	17-Sep-21	4.9	Null pointer dereference	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/1892
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1893
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1894
qca6574a_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1895
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1896
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6574_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1898
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1899
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
qca6584au_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1901
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1902
qca6584_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qca6595au_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1904
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1905
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qca6595_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1907
qca6694au_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1908
qca6694_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://www.qualcomm.com/compan	O-QUA-QCA6-061021/1909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	y/product-security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1910
qca6696_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1911
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P	https://www.qualcomm.	O-QUA-QCA6-061021/1912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	com/company/product-security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-061021/1913
qca7500_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA7-061021/1914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
qca7520_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA7-061021/1915
qca7550_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA7-061021/1916
qca8072_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-QCA8-061021/1917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	-2021-bulletin	
qca8075_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA8-061021/1918
qca8081_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA8-061021/1919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca8337_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA8-061021/1920
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA8-061021/1921
qca9367_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1923
qca9377_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1924
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	O-QUA-QCA9-061021/1925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1926
qca9379_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1927
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qca9531_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1929
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1930
qca9558_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-QCA9-061021/1931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1932
qca9561_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1933
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-QCA9-061021/1934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	-2021-bulletin	
qca9563_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1935
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1936
qca9880_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver	https://www.qualcomm.	O-QUA-QCA9-061021/1937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	com/company/product-security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1938
qca9882_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1939
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P	https://www.qualcomm.	O-QUA-QCA9-061021/1940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	com/company/product-security/bulletins/august-2021-bulletin	
qca9886_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1941
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca9887_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1943
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1944
qca9888_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1946
qca9889_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1947
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qca9896_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1949
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1950
qca9898_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	O-QUA-QCA9-061021/1951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1952
qca9980_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1953
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	O-QUA-QCA9-061021/1954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
qca9982_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1955
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1956
qca9984_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid	https://www.qualcomm.com/compan	O-QUA-QCA9-061021/1957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	y/product-security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1958
qca9985_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1959
qca9986_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1960
qca9987_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1961
qca9988_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qca9990_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1963
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1964
qca9992_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA9-061021/1965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	etins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1966
qca9994_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-061021/1967
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA9-061021/1968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	etins/august-2021-bulletin	
qcm2290_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM2-061021/1969
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM2-061021/1970
qcm4290_firmware					
Use After	17-Sep-21	7.2	Use-after-free vulnerability in	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	QCM4-061021/1971
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM4-061021/1972
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM4-061021/1973
qcm6125_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM6-061021/1974
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM6-061021/1975
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM6-061021/1976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcn3018_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN3-061021/1977
qcn5021_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-061021/1978
qcn5022_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	O-QUA-QCN5-061021/1979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
qcn5024_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-061021/1980
qcn5052_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-061021/1981
qcn5054_firmware					
Use After	17-Sep-21	10	A use after free can occur due	https://ww	O-QUA-QCN5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/1982
qcn5064_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-061021/1983
qcn5121_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	O-QUA-QCN5-061021/1984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qcn5122_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-061021/1985
qcn5124_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-061021/1986
qcn5152_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://www.qualcomm.com/compan	O-QUA-QCN5-061021/1987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	y/product-security/bulletins/august-2021-bulletin	
qcn5154_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-061021/1988
qcn5164_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-061021/1989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
qcn5500_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-061021/1990
qcn5502_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-061021/1991
qcn5550_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-061021/1992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	etins/august-2021-bulletin	
qcn6023_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN6-061021/1993
qcn6024_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN6-061021/1994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcn6122_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN6-061021/1995
qcn9000_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-061021/1996
qcn9012_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	O-QUA-QCN9-061021/1997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	bulletin	
qcn9022_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-061021/1998
qcn9024_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-061021/1999
qcn9070_firmware					
Use After	17-Sep-21	10	A use after free can occur due	https://ww	O-QUA-QCN9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/2000
qcn9072_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-061021/2001
qcn9074_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	O-QUA-QCN9-061021/2002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
qcn9100_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-061021/2003
qcs2290_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS2-061021/2004
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-QCS2-061021/2005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	-2021-bulletin	
qcs405_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-061021/2006
qcs410_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-061021/2007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-061021/2008
qcs4290_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-061021/2009
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-061021/2010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-061021/2011
qcs603_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-061021/2012
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-061021/2013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-061021/2014
qcs605_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-061021/2015
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-061021/2016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-061021/2017
qcs610_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-061021/2018
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-061021/2019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
qcs6125_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-061021/2020
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-061021/2021
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	O-QUA-QCS6-061021/2022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	bulletin	
qcx315_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCX3-061021/2023
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCX3-061021/2024
qet4101_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the	https://www.qualcomm.com/compan	O-QUA-QET4-061021/2025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	y/product-security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QET4-061021/2026
qrb5165_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QRB5-061021/2027
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QRB5-061021/2028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	etins/august-2021-bulletin	
qsm8250_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QSM8-061021/2029
qsw8573_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QSW8-061021/2030
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid	https://www.qualcomm.com/compan	O-QUA-QSW8-061021/2031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	y/product-security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QSW8-061021/2032
qualcomm215_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QUAL-061021/2033
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QUAL-061021/2034

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QUAL-061021/2035
sa415m_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA41-061021/2036
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-SA41-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/2037
sa515m_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA51-061021/2038
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA51-061021/2039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
sa6145p_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2040
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2041
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sa6150p_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2043
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2044
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sa6155p_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2046
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2047
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sa6155_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2049
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2050
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-061021/2051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sa8145p_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-061021/2052
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-061021/2053
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	O-QUA-SA81-061021/2054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	bulletin	
sa8150p_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-061021/2055
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-061021/2056
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SA81-061021/2057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	-2021-bulletin	
sa8155p_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-061021/2058
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-061021/2059
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-061021/2060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	etins/august-2021-bulletin	
sa8155_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-061021/2061
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-061021/2062
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://www.qualcomm.com/company/product-	O-QUA-SA81-061021/2063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	security/bulletins/august-2021-bulletin	
sa8195p_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-061021/2064
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-061021/2065
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://www.qualcomm.com/compan	O-QUA-SA81-061021/2066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	y/product-security/bulletins/august-2021-bulletin	
sc8180x\\+sdx55_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SC81-061021/2067
sd205_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD20-061021/2068
Use After	17-Sep-21	10	A use after free can occur due	https://ww	O-QUA-SD20-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/2069
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD20-061021/2070
sd210_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD21-061021/2071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD21-061021/2072
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD21-061021/2073
sd429_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD42-061021/2074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD42-061021/2075
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD42-061021/2076
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD42-061021/2077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
sd439_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD43-061021/2078
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD43-061021/2079
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD43-061021/2080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sd450_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD45-061021/2081
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD45-061021/2082
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD45-061021/2083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sd460_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD46-061021/2084
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD46-061021/2085
sd480_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	O-QUA-SD48-061021/2086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD48-061021/2087
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD48-061021/2088
sd632_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SD63-061021/2089

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-2021-1939**	-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD63-061021/2090
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD63-061021/2091
sd660_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD66-061021/2092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	etins/august-2021-bulletin	
sd662_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-061021/2093
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-061021/2094
sd665_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the	https://www.qualcomm.com/compan	O-QUA-SD66-061021/2095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	y/product-security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-061021/2096
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-061021/2097
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://www.qualcomm.com/company/product-	O-QUA-SD66-061021/2098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	security/bulletins/august-2021-bulletin	
sd670_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-061021/2099
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-061021/2100
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://www.qualcomm.com/compan	O-QUA-SD67-061021/2101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	y/product-security/bulletins/august-2021-bulletin	
sd675_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-061021/2102
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-061021/2103
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://www.qualcomm.	O-QUA-SD67-061021/2104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	com/company/product-security/bulletins/august-2021-bulletin	
sd678_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-061021/2105
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-061021/2106
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-SD67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/2107
sd690_5g_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD69-061021/2108
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD69-061021/2109
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P	https://www.qualcomm.	O-QUA-SD69-061021/2110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	com/company/product-security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD69-061021/2111
sd712_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD71-061021/2112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd720g_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD72-061021/2113
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD72-061021/2114
sd730_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD73-061021/2115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD73-061021/2116
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD73-061021/2117
sd750g_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD75-061021/2118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD75-061021/2119
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD75-061021/2120
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD75-061021/2121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sd765g_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2122
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2123
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2125
sd765_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2126
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1947**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2128
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2129
sd768g_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2131
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2132
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-061021/2133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sd778g_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD77-061021/2134
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD77-061021/2135
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD77-061021/2136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sd780g_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD78-061021/2137
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD78-061021/2138
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD78-061021/2139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
sd820_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD82-061021/2140
sd821_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD82-061021/2141
sd835_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD83-061021/2142

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD83-061021/2143
sd845_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD84-061021/2144
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://www.qualcomm.com/compan	O-QUA-SD84-061021/2145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	y/product-security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD84-061021/2146
sd850_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-061021/2147
sd855_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-061021/2148
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-061021/2149
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-061021/2150
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-SD85-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/2151
sd865_5g_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD86-061021/2152
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD86-061021/2153
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P	https://www.qualcomm.	O-QUA-SD86-061021/2154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	com/company/product-security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD86-061021/2155
sd870_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD87-061021/2156
Use After	17-Sep-21	7.2	Use-after-free vulnerability in	https://ww	O-QUA-SD87-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/2157
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD87-061021/2158
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD87-061021/2159
sd888_5g_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD88-061021/2160
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD88-061021/2161
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD88-061021/2162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd888_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD88-061021/2163
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD88-061021/2164
sda429w_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDA4-061021/2165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDA4-061021/2166
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDA4-061021/2167
sdm429w_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM4-061021/2168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM4-061021/2169
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM4-061021/2170
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM4-061021/2171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdm630_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM6-061021/2172
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM6-061021/2173
sdm830_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM8-061021/2174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM8-061021/2175
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM8-061021/2176
sdw2500_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	O-QUA-SDW2-061021/2177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDW2-061021/2178
sdx12_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX1-061021/2179
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	O-QUA-SDX1-061021/2180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	bulletin	
sdx20m_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-061021/2181
sdx20_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-061021/2182
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://www.qualcomm.	O-QUA-SDX2-061021/2183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	com/company/product-security/bulletins/august-2021-bulletin	
sdx24_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-061021/2184
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-061021/2185
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/2186
sdx50m_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-061021/2187
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-061021/2188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
sdx55m_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-061021/2189
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-061021/2190
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-061021/2191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-061021/2192
sdx55_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-061021/2193
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-061021/2194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-061021/2195
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-061021/2196
sdxr1_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-061021/2197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-061021/2198
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-061021/2199
sdxr2_5g_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-061021/2200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-061021/2201
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-061021/2202
sd_455_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_4-061021/2203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_4-061021/2204
sd_636_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_6-061021/2205
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-SD_6-061021/2206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	-2021-bulletin	
sd_675_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_6-061021/2207
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_6-061021/2208
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD_6-061021/2209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	etins/august-2021-bulletin	
sd_8cx_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_8-061021/2210
sd_8c_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_8-061021/2211
sm4125_firmware					
NULL	17-Sep-21	4.9	Null pointer dereference	https://ww	O-QUA-SM41-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/2212
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM41-061021/2213
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM41-061021/2214
sm6250p_firmware					
Use After	17-Sep-21	10	A use after free can occur due	https://ww	O-QUA-SM62-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	061021/2215
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-061021/2216
sm6250_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-061021/2217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-061021/2218
sm7250_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM72-061021/2219
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM72-061021/2220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM72-061021/2221
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM72-061021/2222
sm7325_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM73-061021/2223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1939**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM73-061021/2224
wcd9306_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2225
wcd9326_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	O-QUA-WCD9-061021/2226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	bulletin	
wcd9330_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2227
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2228
wcd9335_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature	https://www.qualcomm.com/company/product-	O-QUA-WCD9-061021/2229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2230
wcd9340_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2231
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-WCD9-061021/2232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2233
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2234
wcd9341_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-061021/2235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	etins/august-2021-bulletin	
wcd9360_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2236
wcd9370_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2237
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-WCD9-061021/2238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2239
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2240
wcd9371_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the	https://www.qualcomm.com/compan	O-QUA-WCD9-061021/2241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	y/product-security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2242
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2243
wcd9375_firmware					
NULL Pointer	17-Sep-21	4.9	Null pointer dereference occurs due to improper	https://www.qualcomm.	O-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	com/company/product-security/bulletins/august-2021-bulletin	061021/2244
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2245
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2246
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://www.qualcomm.com/compan	O-QUA-WCD9-061021/2247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	y/product-security/bulletins/august-2021-bulletin	
wcd9380_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2248
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2249
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-WCD9-061021/2250

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2251
wcd9385_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2252
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid	https://www.qualcomm.com/compan	O-QUA-WCD9-061021/2253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	y/product-security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2254
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-061021/2255
wcn3610_firmware					
NULL Pointer	17-Sep-21	4.9	Null pointer dereference occurs due to improper	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	com/company/product-security/bulletins/august-2021-bulletin	061021/2256
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2257
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2258
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://www.qualcomm.com/compan	O-QUA-WCN3-061021/2259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	y/product-security/bulletins/august-2021-bulletin	
wcn3615_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2260
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2261
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-WCN3-061021/2262

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, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2263
wcn3620_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2264
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid	https://www.qualcomm.com/compan	O-QUA-WCN3-061021/2265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	y/product-security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2266
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2267
wcn3660b_firmware					
NULL Pointer	17-Sep-21	4.9	Null pointer dereference occurs due to improper	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	com/company/product-security/bulletins/august-2021-bulletin	061021/2268
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2269
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2270
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://www.qualcomm.com/compan	O-QUA-WCN3-061021/2271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	y/product-security/bulletins/august-2021-bulletin	
wcn3660_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2272
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2273
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	com/company/product-security/bulletins/august-2021-bulletin	061021/2274
wcn3680b_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2275
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2276
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://www.qualcomm.com/compan	O-QUA-WCN3-061021/2277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	y/product-security/bulletins/august-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2278
wcn3680_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2279
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	com/company/product-security/bulletins/august-2021-bulletin	061021/2280
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2281
wcn3910_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2282
Use After	17-Sep-21	7.2	Use-after-free vulnerability in	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	WCN3-061021/2283
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2284
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2285
wcn3950_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2286
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2287
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2288
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	w.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	WCN3-061021/2289
wcn3980_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2290
wcn3988_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2292
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2293
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wcn3990_firmware					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2295
wcn3991_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2296
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2298
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2299
wcn3998_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2301
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2302
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
wcn3999_firmware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-061021/2304
wcn6740_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2305
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame 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/august-2021-bulletin	O-QUA-WCN6-061021/2306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2307
wcn6750_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2308
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2310
wcn6850_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2311
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2313
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2314
wcn6851_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-	O-QUA-WCN6-061021/2315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2316
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2317
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**		
wcn6855_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2319
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2320
wcn6856_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-WCN6-061021/2321

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-2021-1939**	-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2322
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-061021/2323
whs9410_firmware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://www.qualcomm.com/company/product-security/bull	O-QUA-WHS9-061021/2324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	etins/august-2021-bulletin	
wsa8810_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-061021/2325
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-061021/2326
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-WSA8-061021/2327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-061021/2328
wsa8815_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-061021/2329
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-WSA8-061021/2330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	etins/august-2021-bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-061021/2331
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-061021/2332
wsa8830_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature	https://www.qualcomm.com/company/product-	O-QUA-WSA8-061021/2333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	security/bulletins/august-2021-bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-061021/2334
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-061021/2335
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://www.qualcomm.com/company/product-security/bull	O-QUA-WSA8-061021/2336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	etins/august-2021-bulletin	
wsa8835_firmware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2021-1939**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-061021/2337
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1947**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-061021/2338
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/august	O-QUA-WSA8-061021/2339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1976**	-2021-bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-30261**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-061021/2340
Zyxel					
zywall_vpn2s_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Sep-21	5	A directory traversal vulnerability in the web server of the Zyxel VPN2S firmware version 1.12 could allow a remote attacker to gain access to sensitive information. **CVE ID : CVE-2021-35027**	https://www.zyxel.com/support/Zyxel_security_advisory_for_directory_traversal_and_command_injection_vulnerabilities_of_VPN2S_Firewall.shtml	O-ZYX-ZYWA-061021/2341
Improper Neutralization of Special Elements	29-Sep-21	7.2	A command injection vulnerability in the CGI program of the Zyxel VPN2S firmware version 1.12 could	https://www.zyxel.com/support/Zyxel_security_a	O-ZYX-ZYWA-061021/2342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			allow an authenticated, local user to execute arbitrary OS commands. **CVE ID : CVE-2021-35028**	dvisory_for_directory_traversal_and_command_injection_vulnerabilities_of_VPN2S_Firewall.shtml	