Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Accusoft					
imagegear					
Out-of-bounds Write	08-Jul-21	6.8	An out-of-bounds write vulnerability exists in the JPG sof_nb_comp header processing functionality of Accusoft ImageGear 19.8 and 19.9. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21793**	N/A	A-ACC-IMAG-200721/1
Out-of-bounds Write	08-Jul-21	6.8	An out-of-bounds write vulnerability exists in the TIF bits_per_sample processing functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21794**	N/A	A-ACC-IMAG-200721/2
Integer Overflow or Wraparound	07-Jul-21	6.8	An integer overflow vulnerability exists in the DICOM parse_dicom_meta_info functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to a stack-based buffer	N/A	A-ACC-IMAG-200721/3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21807**		
Out-of-bounds Write	08-Jul-21	6.8	A stack-based buffer overflow vulnerability exists in the PDF process_fontname functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21821**	N/A	A-ACC-IMAG-200721/4
addressable_project					
addressable					
Uncontrolled Resource Consumption	06-Jul-21	5	Addressable is an alternative implementation to the URI implementation that is part of Ruby's standard library. An uncontrolled resource consumption vulnerability exists after version 2.3.0 through version 2.7.0. Within the URI template implementation in Addressable, a maliciously crafted template may result in uncontrolled resource consumption, leading to denial of service when matched against a URI. In typical usage, templates would not normally be read from untrusted user input, but nonetheless, no previous security advisory for Addressable has cautioned	https://github.com/sporkmonger/addressable/security/advisories/GHSA-jxhc-q857-3j6g, https://github.com/sporkmonger/addressable/commit/0d8a3127e35886ce9284810a7f2438bff6b43cbc	A-ADD-ADDR-200721/5

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			against doing this. Users of the parsing capabilities in Addressable but not the URI template capabilities are unaffected. The vulnerability is patched in version 2.8.0. As a workaround, only create Template objects from trusted sources that have been validated not to produce catastrophic backtracking. **CVE ID : CVE-2021-32740**		
admincolumns					
admin_columns					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	3.5	The Admin Columns WordPress plugin Free before 4.3.2 and Pro before 5.5.2 allowed to configure individual columns for tables. Each column had a type. The type "Custom Field" allowed to choose an arbitrary database column to display in the table. There was no escaping applied to the contents of "Custom Field" columns. **CVE ID : CVE-2021-24365**	https://wpscan.com/vulnerability/fdbeb137-b404-46c7-85fb-394a3bdac388	A-ADM-ADMI-200721/6
alpinelinux					
aports					
Cleartext Storage of Sensitive Information	05-Jul-21	4.3	In the xrdp package (in branches through 3.14) for Alpine Linux, RDP sessions are vulnerable to man-in-the-middle attacks because pre-generated RSA certificates and private keys	https://gitlab.alpinelinux.org/alpine/aports/-/issues/12811	A-ALP-APOR-200721/7

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are used. **CVE ID : CVE-2021-36158**		
Apache					
druid					
Incorrect Authorization	02-Jul-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 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. **CVE ID : CVE-2021-26920**	https://lists.apache.org/thread.html/r29e45561343cc5cf7d3290ee0b0e94e565faab19c20d022df9b5e29c%40%3Cdev.druid.apache.org%3E, https://lists.apache.org/thread.html/r61aab724cf97d80da7f02d50e9af6de5c7c40dd92dab7518746fbaa2@%3Cannounce.apache.org%3E	A-APA-DRUI-200721/8
jena_fuseki					
Improper Neutralization of Input During Web Page	05-Jul-21	4.3	A vulnerability in the HTML pages of Apache Jena Fuseki allows an attacker to execute arbitrary javascript on certain page views. This	https://lists.apache.org/thread.html/r684d8943d755a96fe90f8	A-APA-JENA-200721/9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			issue affects Apache Jena Fuseki from version 2.0.0 to version 4.0.0 (inclusive). **CVE ID : CVE-2021-33192**	cd8df196737b6bde3f2b74e15a9bd479975%40%3Cusers.jena.apache.org%3E	
tomcat					
Improper Handling of Exceptional Conditions	12-Jul-21	5	A vulnerability in Apache Tomcat allows an attacker to remotely trigger a denial of service. An error introduced as part of a change to improve error handling during non-blocking I/O meant that the error flag associated with the Request object was not reset between requests. This meant that once a non-blocking I/O error occurred, all future requests handled by that request object would fail. Users were able to trigger non-blocking I/O errors, e.g. by dropping a connection, thereby creating the possibility of triggering a DoS. Applications that do not use non-blocking I/O are not exposed to this vulnerability. This issue affects Apache Tomcat 10.0.3 to 10.0.4; 9.0.44; 8.5.64. **CVE ID : CVE-2021-30639**	https://lists.apache.org/thread.html/rd84fae1f474597bdf358f5bdc0a5c453c507bd527b83e8be6b5ea3f4%40%3Cannounce.tomcat.apache.org%3E	A-APA-TOMC-200721/10
Inconsistent Interpretation of HTTP Requests ('HTTP Request	12-Jul-21	5	Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some	https://lists.apache.org/thread.html/r612a79269b0d5e5780c62dfd34286a	A-APA-TOMC-200721/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Smuggling')			circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding. **CVE ID : CVE-2021-33037**	8037232fec0bc6f1a7e60c9381%40%3Cannounce.tomcat.apache.org%3E	
artware_cms_project					
artware_cms					
Unrestricted Upload of File with Dangerous Type	07-Jul-21	7.5	ARTWARE CMS parameter of image upload function does not filter the type of upload files which allows remote attackers can upload arbitrary files without logging in, and further execute code unrestrictedly. **CVE ID : CVE-2021-32538**	https://www.twcert.org.tw/tw/cp-132-4850-9b53f-1.html	A-ART-ARTW-200721/12
Arubanetworks					
clearpass_policy_manager					
Deserialization of Untrusted Data	08-Jul-21	9	A remote insecure deserialization vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt	A-ARU-CLEA-200721/13

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29150		
Improper Authentication	08-Jul-21	4	A remote authentication bypass vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2021-29151**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt	A-ARU-CLEA-200721/14
Uncontrolled Resource Consumption	08-Jul-21	6.8	A remote denial of service (DoS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2021-29152**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt	A-ARU-CLEA-200721/15
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jul-21	6.5	A remote SQL injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2021-34609**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt	A-ARU-CLEA-200721/16
Improper Neutralization of Special Elements used in a Command	08-Jul-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt	A-ARU-CLEA-200721/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			has released updates to ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2021-34610**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Jul-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2021-34611**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt	A-ARU-CLEA-200721/18
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Jul-21	6.5	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2021-34612**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt	A-ARU-CLEA-200721/19
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Jul-21	6.5	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2021-34613**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt	A-ARU-CLEA-200721/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Jul-21	6.5	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2021-34614**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt	A-ARU-CLEA-200721/21
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Jul-21	6.5	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2021-34615**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt	A-ARU-CLEA-200721/22
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Jul-21	6.5	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2021-34616**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt	A-ARU-CLEA-200721/23
Autodesk					
design_review					
Out-of-bounds Write	09-Jul-21	6.8	A heap-based buffer overflow could occur while parsing PICT or TIFF files in	https://www.autodesk.com/trust/se	A-AUT-DESI-200721/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Autodesk 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2021-27034**	curity-advisories/adsk-sa-2021-0003	
Out-of-bounds Write	09-Jul-21	6.8	A maliciously crafted TIFF, PDF, PICT or DWF files in Autodesk 2018, 2017, 2013, 2012, 2011 can be forced to read beyond allocated boundaries when parsing the TIFF, PDF, PICT or DWF files. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2021-27035**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2021-0003	A-AUT-DESI-200721/25
Out-of-bounds Write	09-Jul-21	6.8	A maliciously crafted PDF, PICT or TIFF file can be used to write beyond the allocated buffer while parsing PDF, PICT or TIFF files in Autodesk 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2021-27036**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2021-0003	A-AUT-DESI-200721/26
Use After Free	09-Jul-21	6.8	A maliciously crafted PNG, PDF or DWF file in Autodesk 2018, 2017, 2013, 2012, 2011 can be used to attempt to free an object that has already been freed while parsing them. This vulnerability can be exploited by remote attackers to execute arbitrary code.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2021-0003	A-AUT-DESI-200721/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27037		
Access of Resource Using Incompatible Type ('Type Confusion')	09-Jul-21	6.8	A Type Confusion vulnerability in Autodesk 2018, 2017, 2013, 2012, 2011 can occur when processing a maliciously crafted PDF file. An attacker can leverage this to execute arbitrary code. **CVE ID : CVE-2021-27038**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2021-0003	A-AUT-DESI-200721/28
Out-of-bounds Write	09-Jul-21	6.8	A maliciously crafted TIFF file in Autodesk 2018, 2017, 2013, 2012, 2011 can be forced to read and write beyond allocated boundaries when parsing the TIFF file. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2021-27039**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2021-0003	A-AUT-DESI-200721/29
Avahi					
avahi					
NULL Pointer Dereference	07-Jul-21	2.1	Avahi 0.8 allows a local denial of service (NULL pointer dereference and daemon crash) against avahi-daemon via the D-Bus interface or a "ping .local" command. **CVE ID : CVE-2021-36217**	https://github.com/lathiat/avahi/commit/9d31939e55280a733d930b15ac9e4dda4497680c	A-AVA-AVAH-200721/30
beardev					
joomsport					
Deserialization of Untrusted Data	06-Jul-21	7.5	The joomsport_md_load AJAX action of the JoomSport WordPress plugin before 5.1.8, registered for both unauthenticated and	https://wpscan.com/vulnerability/fb6c407c-713c-4e83-92ce-	A-BEA-JOOM-200721/31

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated users, unserialised user input from the shattr POST parameter, leading to a PHP Object Injection issue. Even though the plugin does not have a suitable gadget chain to exploit this, other installed plugins could, which might lead to more severe issues such as RCE **CVE ID : CVE-2021-24384**	4e5f791be696	
boldgrid					
w3_total_cache					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	3.5	The W3 Total Cache WordPress plugin before 2.1.3 did not sanitise or escape some of its CDN settings, allowing high privilege users to use JavaScript in them, which will be output in the page, leading to an authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24427**	https://wpscan.com/vulnerability/5da5ce9a-82a6-404f-8dec-795d7905b3f9	A-BOL-W3_T-200721/32
Brave					
brave					
Exposure of Sensitive Information to an Unauthorized Actor	12-Jul-21	4.3	In Brave Desktop between versions 1.17 and 1.26.60, when adblocking is enabled and a proxy browser extension is installed, the CNAME adblocking feature issues DNS requests that used the system DNS settings instead of the extension's proxy settings,	N/A	A-BRA-BRAV-200721/33

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in possible information disclosure. **CVE ID : CVE-2021-22916**		
browser					
Exposure of Sensitive Information to an Unauthorized Actor	12-Jul-21	4.3	Brave Browser Desktop between versions 1.17 and 1.20 is vulnerable to information disclosure by way of DNS requests in Tor windows not flowing through Tor if adblocking was enabled. **CVE ID : CVE-2021-22917**	N/A	A-BRA-BROW-200721/34
chimpgroup					
foodbakery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-21	4.3	The WP Foodbakery WordPress plugin before 2.2, used in the FoodBakery WordPress theme before 2.2 did not properly sanitize the foodbakery_radius parameter before outputting it back in the response, leading to an unauthenticated Reflected Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2021-24389**	https://wpscan.com/vulnerability/23b8b8c4-cded-4887-a021-5f3ea610213b	A-CHI-FOOD-200721/35
Cisco					
adaptive_security_device_manager					
Improper Control of Generation of Code ('Code Injection')	08-Jul-21	9.3	A vulnerability in the Cisco Adaptive Security Device Manager (ASDM) Launcher could allow an unauthenticated, remote attacker to execute arbitrary code on a user's operating	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-	A-CIS-ADAP-200721/36

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system. This vulnerability is due to a lack of proper signature verification for specific code exchanged between the ASDM and the Launcher. An attacker could exploit this vulnerability by leveraging a man-in-the-middle position on the network to intercept the traffic between the Launcher and the ASDM and then inject arbitrary code. A successful exploit could allow the attacker to execute arbitrary code on the user's operating system with the level of privileges assigned to the ASDM Launcher. A successful exploit may require the attacker to perform a social engineering attack to persuade the user to initiate communication from the Launcher to the ASDM. **CVE ID : CVE-2021-1585**	gqjShXW	
broadworks_application_server					
Exposure of Sensitive Information to an Unauthorized Actor	08-Jul-21	4	A vulnerability in the XSI-Actions interface of Cisco BroadWorks Application Server could allow an authenticated, remote attacker to access sensitive information on an affected system. This vulnerability is due to improper input validation and authorization of specific commands that a user can execute within the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broad-as-inf-disc-ZUXGFFXQ	A-CIS-BROA-200721/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			XSI-Actions interface. An attacker could exploit this vulnerability by authenticating to an affected device and issuing a specific set of commands. A successful exploit could allow the attacker to join a Call Center instance and have calls that they do not have permissions to access distributed to them from the Call Center queue. At the time of publication, Cisco had not released updates that address this vulnerability for Cisco BroadWorks Application Server. However, firmware patches are available. **CVE ID : CVE-2021-1562**		
business_process_automation					
Use of Hard-coded Credentials	08-Jul-21	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Business Process Automation (BPA) could allow an authenticated, remote attacker to elevate privileges to Administrator. These vulnerabilities are due to improper authorization enforcement for specific features and for access to log files that contain confidential information. An attacker could exploit these vulnerabilities either by submitting crafted HTTP messages to an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bpa-priv-esc-dgubwbH4	A-CIS-BUSI-200721/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system and performing unauthorized actions with the privileges of an administrator, or by retrieving sensitive data from the logs and using it to impersonate a legitimate privileged user. A successful exploit could allow the attacker to elevate privileges to Administrator. **CVE ID : CVE-2021-1574**		
Insertion of Sensitive Information into Log File	08-Jul-21	4	Multiple vulnerabilities in the web-based management interface of Cisco Business Process Automation (BPA) could allow an authenticated, remote attacker to elevate privileges to Administrator. These vulnerabilities are due to improper authorization enforcement for specific features and for access to log files that contain confidential information. An attacker could exploit these vulnerabilities either by submitting crafted HTTP messages to an affected system and performing unauthorized actions with the privileges of an administrator, or by retrieving sensitive data from the logs and using it to impersonate a legitimate privileged user. A successful exploit could allow the attacker to elevate privileges	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bpa-priv-esc-dgubwbH4	A-CIS-BUSI-200721/39

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to Administrator. **CVE ID : CVE-2021-1576**		
identity_services_engine					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials. **CVE ID : CVE-2021-1603**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stored-xss-TWwjVPdL	A-CIS-IDEN-200721/40
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stored-xss-	A-CIS-IDEN-200721/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials. **CVE ID : CVE-2021-1604**	TWwjVPdL	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stored-xss-TWwjVPdL	A-CIS-IDEN-200721/42

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials. **CVE ID : CVE-2021-1605**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials. **CVE ID : CVE-2021-1606**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stored-xss-TWwjVPdL	A-CIS-IDEN-200721/43
Improper Neutralization of Input During Web	08-Jul-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could	https://tools.cisco.com/security/center/content/Cis	A-CIS-IDEN-200721/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials. **CVE ID : CVE-2021-1607**	coSecurityAdvisory/cisco-sa-ise-stored-xss-TWwjVPdL	
virtualized_voice_browser					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jul-21	4.3	A vulnerability in the web-based management interface of Cisco Virtualized Voice Browser could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vvb-xss-wG4zXRp3	A-CIS-VIRT-200721/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2021-1575**		
web_security_appliance					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Jul-21	9	A vulnerability in the configuration management of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to perform command injection and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied XML input for the web interface. An attacker could exploit this vulnerability by uploading crafted XML configuration files that contain scripting code to a vulnerable device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root. An attacker would need a valid user account with the rights to upload configuration files to exploit this vulnerability. **CVE ID : CVE-2021-1359**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-scr-web-priv-esc-k3HCGJZ	A-CIS-WEB_-200721/46

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
codeblab					
glass					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	4.3	The Glass WordPress plugin through 1.3.2 does not sanitise or escape its "Glass Pages" setting before outputting in a page, leading to a Stored Cross-Site Scripting issue. Furthermore, the plugin did not have CSRF check in place when saving its settings, allowing the issue to be exploited via a CSRF attack. **CVE ID : CVE-2021-24434**	https://wpscan.com/vulnerability/dbea2dc2-83f6-4e70-b044-a68a4c9b9c39	A-COD-GLAS-200721/47
codemiq					
wordpress_email_template_designer					
Cross-Site Request Forgery (CSRF)	07-Jul-21	6.8	Cross-site request forgery (CSRF) vulnerability in WordPress Email Template Designer - WP HTML Mail versions prior to 3.0.8 allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2021-20779**	N/A	A-COD-WORD-200721/48
commscope					
ruckus_iot_controller					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jul-21	4	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. The API allows Directory Traversal. **CVE ID : CVE-2021-33215**	N/A	A-COM-RUCK-200721/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Jul-21	7.5	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. An Undocumented Backdoor exists, allowing shell access via a developer account. **CVE ID : CVE-2021-33216**	N/A	A-COM-RUCK-200721/50
Out-of-bounds Write	07-Jul-21	9	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. The Web Application allows Arbitrary Read/Write actions by authenticated users. The API allows an HTTP POST of arbitrary content into any file on the filesystem as root. **CVE ID : CVE-2021-33217**	N/A	A-COM-RUCK-200721/51
Use of Hard-coded Credentials	07-Jul-21	10	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. There are Hard-coded System Passwords that provide shell access. **CVE ID : CVE-2021-33218**	N/A	A-COM-RUCK-200721/52
Use of Hard-coded Credentials	07-Jul-21	7.5	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. There are Hard-coded Web Application Administrator Passwords for the admin and nplus1user accounts. **CVE ID : CVE-2021-33219**	N/A	A-COM-RUCK-200721/53
Use of Hard-coded Credentials	07-Jul-21	4.6	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. Hard-coded API Keys	N/A	A-COM-RUCK-200721/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exist. **CVE ID : CVE-2021-33220**		
Missing Authentication for Critical Function	07-Jul-21	7.5	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. There are Unauthenticated API Endpoints. **CVE ID : CVE-2021-33221**	N/A	A-COM-RUCK-200721/55
contempothemes					
real_estate_7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-21	4.3	The WP Pro Real Estate 7 WordPress theme before 3.1.1 did not properly sanitise the ct_community parameter in its search listing page before outputting it back in it, leading to a reflected Cross-Site Scripting which can be triggered in both unauthenticated or authenticated user context **CVE ID : CVE-2021-24387**	https://wpscan.com/vulnerability/27264f30-71d5-4d2b-8f36-4009a2be6745, https://contempothemes.com/wp-real-estate-7/changelog/	A-CON-REAL-200721/56
deliciousbrains					
wp_offload_ses_lite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-21	3.5	The WP Offload SES Lite WordPress plugin before 1.4.5 did not escape some of the fields in the Activity page of the admin dashboard, such as the email's id, subject and recipient, which could lead to Stored Cross-Site Scripting issues when an attacker can control any of these fields, like the subject when filling a contact form	https://wpscan.com/vulnerability/8f14733e-84c3-4f7c-93f8-e27c74519160	A-DEL-WP_O-200721/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for example. The XSS will be executed in the context of a logged in admin viewing the Activity tab of the plugin. **CVE ID : CVE-2021-24494**		
Dell					
emc_unityvsa_operating_environment					
N/A	12-Jul-21	4.6	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 do not exit on failed Initialization. A local authenticated Service user could potentially exploit this vulnerability to escalate privileges. **CVE ID : CVE-2021-21589**	https://www.dell.com/support/kbdoc/000189204	A-DEL-EMC_-200721/58
Exposure of Sensitive Information to an Unauthorized Actor	12-Jul-21	4.6	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user. **CVE ID : CVE-2021-21590**	https://www.dell.com/support/kbdoc/000189204	A-DEL-EMC_-200721/59
Exposure of Sensitive Information to an Unauthorized Actor	12-Jul-21	4.6	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user. **CVE ID : CVE-2021-21591**	https://www.dell.com/support/kbdoc/000189204	A-DEL-EMC_-200721/60

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
emc_unity_operating_environment					
N/A	12-Jul-21	4.6	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 do not exit on failed Initialization. A local authenticated Service user could potentially exploit this vulnerability to escalate privileges. **CVE ID : CVE-2021-21589**	https://www.dell.com/support/kbdoc/000189204	A-DEL-EMC_-200721/61
Exposure of Sensitive Information to an Unauthorized Actor	12-Jul-21	4.6	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user. **CVE ID : CVE-2021-21590**	https://www.dell.com/support/kbdoc/000189204	A-DEL-EMC_-200721/62
Exposure of Sensitive Information to an Unauthorized Actor	12-Jul-21	4.6	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user. **CVE ID : CVE-2021-21591**	https://www.dell.com/support/kbdoc/000189204	A-DEL-EMC_-200721/63
emc_unity_xt_operating_environment					
N/A	12-Jul-21	4.6	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 do not exit on failed Initialization. A local authenticated Service	https://www.dell.com/support/kbdoc/000189204	A-DEL-EMC_-200721/64

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user could potentially exploit this vulnerability to escalate privileges. **CVE ID : CVE-2021-21589**		
Exposure of Sensitive Information to an Unauthorized Actor	12-Jul-21	4.6	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user. **CVE ID : CVE-2021-21590**	https://www.dell.com/support/kbdoc/000189204	A-DEL-EMC_-200721/65
Exposure of Sensitive Information to an Unauthorized Actor	12-Jul-21	4.6	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user. **CVE ID : CVE-2021-21591**	https://www.dell.com/support/kbdoc/000189204	A-DEL-EMC_-200721/66
powerflex_presentation_server					
Insufficient Verification of Data Authenticity	12-Jul-21	4.3	Dell EMC PowerFlex, v3.5.x contain a Cross-Site WebSocket Hijacking Vulnerability in the Presentation Server/WebUI. An unauthenticated attacker could potentially exploit this vulnerability by tricking the user into performing unwanted actions on the Presentation Server and perform which may lead to	https://www.dell.com/support/kbdoc/000189265	A-DEL-POWE-200721/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration changes. **CVE ID : CVE-2021-21588**		
deltaww					
dopsoft					
Out-of-bounds Read	02-Jul-21	6.8	Delta Electronics DOPSoft Versions 4.0.10.17 and prior are vulnerable to an out-of-bounds read, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2021-27412**	N/A	A-DEL-DOPS-200721/68
Out-of-bounds Read	02-Jul-21	4.3	Delta Electronics DOPSoft Versions 4.0.10.17 and prior are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to disclose information. **CVE ID : CVE-2021-27455**	N/A	A-DEL-DOPS-200721/69
devolutions					
devolutions_server					
Improper Certificate Validation	12-Jul-21	4.3	Devolutions Server before 2021.1.18, and LTS before 2020.3.20, allows attackers to intercept private keys via a man-in-the-middle attack against the connections/partial endpoint (which accepts cleartext). **CVE ID : CVE-2021-36382**	https://devolutions.net/security/advisories/DEVO-2021-0005	A-DEV-DEVO-200721/70
Djangoproject					
django					
Improper Neutralization of Special	02-Jul-21	7.5	Django 3.1.x before 3.1.13 and 3.2.x before 3.2.5 allows QuerySet.order_by SQL	https://docs.djangoproject.com/en/3.2	A-DJA-DJAN-200721/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			injection if order_by is untrusted input from a client of a web application. **CVE ID : CVE-2021-35042**	/releases/security/, https://www.openwall.com/lists/oss-security/2021/07/02/2, https://www.djangoproject.com/weblog/2021/jul/01/security-releases/	
Dotcms					
dotcms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-21	3.5	A stored cross site scripting (XSS) vulnerability in dotAdmin/#/c/c_Images of dotCMS 21.05.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' and 'Filename' parameters. **CVE ID : CVE-2021-35358**	N/A	A-DOT-DOTC-200721/72
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-21	3.5	A reflected cross site scripting (XSS) vulnerability in dotAdmin/#/c/containers of dotCMS 21.05.1 allows attackers to execute arbitrary commands or HTML via a crafted payload. **CVE ID : CVE-2021-35360**	N/A	A-DOT-DOTC-200721/73
Improper Neutralization of Input During Web	09-Jul-21	3.5	A reflected cross site scripting (XSS) vulnerability in dotAdmin/#/c/links of dotCMS 21.05.1 allows	N/A	A-DOT-DOTC-200721/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			attackers to execute arbitrary commands or HTML via a crafted payload. **CVE ID : CVE-2021-35361**		
e4j					
vikrentcar_car_rental_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-21	3.5	In the VikRentCar Car Rental Management System WordPress plugin before 1.1.7, there is a custom filed option by which we can manage all the fields that the users will have to fill in before saving the order. However, the field name is not sanitised or escaped before being output back in the page, leading to a stored Cross-Site Scripting issue. There is also no CSRF check done before saving the setting, allowing attackers to make a logged in admin set arbitrary Custom Fields, including one with XSS payload in it. **CVE ID : CVE-2021-24388**	https://wpscan.com/vulnerability/e3f6576f-08cb-4278-8c79-3ef4d0b85cd9	A-E4J-VIKR-200721/75
Ec-cube					
ec-cube					
N/A	01-Jul-21	5	Improper access control vulnerability in EC-CUBE 4.0.6 (EC-CUBE 4 series) allows a remote attacker to bypass access restriction and obtain sensitive information via unspecified vectors. **CVE ID : CVE-2021-20778**	https://www.ec-cube.net/info/weakness/weakness.php?id=80	A-EC--EC-C-200721/76

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
echobh					
sharecare					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Jul-21	7.5	Echo ShareCare 8.15.5 is susceptible to SQL injection vulnerabilities when processing remote input from both authenticated and unauthenticated users, leading to the ability to bypass authentication, exfiltrate Structured Query Language (SQL) records, and manipulate data. **CVE ID : CVE-2021-33578**	N/A	A-ECH-SHAR-200721/77
Unrestricted Upload of File with Dangerous Type	13-Jul-21	6.5	An issue was discovered in Echo ShareCare 8.15.5. The file-upload feature in Access/DownloadFeed_Mnt/FileUpload_Upd.cfm is susceptible to an unrestricted upload vulnerability via the name1 parameter, when processing remote input from an authenticated user, leading to the ability for arbitrary files to be written to arbitrary filesystem locations via ../ Directory Traversal on the Z: drive (a hard-coded drive letter where ShareCare application files reside) and remote code execution as the ShareCare service user (NT AUTHORITY\SYSTEM). **CVE ID : CVE-2021-36121**	N/A	A-ECH-SHAR-200721/78
Improper Neutralizatio	13-Jul-21	6.5	An issue was discovered in Echo ShareCare 8.15.5. The	N/A	A-ECH-SHAR-200721/79

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Argument Delimiters in a Command ('Argument Injection')			UnzipFile feature in Access/EligFeedParse_Sup/UnzipFile_Upd.cfm is susceptible to a command argument injection vulnerability when processing remote input in the zippass parameter from an authenticated user, leading to the ability to inject arbitrary arguments to 7z.exe. **CVE ID : CVE-2021-36122**		
N/A	13-Jul-21	4	An issue was discovered in Echo ShareCare 8.15.5. The TextReader feature in General/TextReader/TextReader.cfm is susceptible to a local file inclusion vulnerability when processing remote input in the textFile parameter from an authenticated user, leading to the ability to read arbitrary files on the server filesystems as well any files accessible via Universal Naming Convention (UNC) paths. **CVE ID : CVE-2021-36123**	N/A	A-ECH-SHAR-200721/80
Improper Authentication	13-Jul-21	7.5	An issue was discovered in Echo ShareCare 8.15.5. It does not perform authentication or authorization checks when accessing a subset of sensitive resources, leading to the ability for unauthenticated users to access pages that are	N/A	A-ECH-SHAR-200721/81

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to attacks such as SQL injection. **CVE ID : CVE-2021-36124**		
Eclipse					
tinydtls					
Inadequate Encryption Strength	08-Jul-21	5	Eclipse TinyDTLS through 0.9-rc1 relies on the rand function in the C library, which makes it easier for remote attackers to compute the master key and then decrypt DTLS traffic. **CVE ID : CVE-2021-34430**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=568803	A-ECL-TINY-200721/82
edgexfoundry					
edgex_foundry					
Weak Password Requirements	09-Jul-21	5.8	EdgeX Foundry is an open source project for building a common open framework for internet-of-things edge computing. A vulnerability exists in the Edinburgh, Fuji, Geneva, and Hanoi versions of the software. When the EdgeX API gateway is configured for OAuth2 authentication and a proxy user is created, the client_id and client_secret required to obtain an OAuth2 authentication token are set to the username of the proxy user. A remote network attacker can then perform a dictionary-based password attack on the OAuth2 token endpoint of the API gateway to obtain an OAuth2 authentication token and use	https://github.com/edgexfoundry/edgex-go/security/advisories/GHSA-xph4-vmcc-52gh	A-EDG-EDGE-200721/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that token to make authenticated calls to EdgeX microservices from an untrusted network. OAuth2 is the default authentication method in EdgeX Edinburgh release. The default authentication method was changed to JWT in Fuji and later releases. Users should upgrade to the EdgeX Ireland release to obtain the fix. The OAuth2 authentication method is disabled in Ireland release. If unable to upgrade and OAuth2 authentication is required, users should create OAuth2 users directly using the Kong admin API and forgo the use of the `security-proxy-setup` tool to create OAuth2 users. **CVE ID : CVE-2021-32753**		
edifecs					
transaction_management					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Jul-21	5	In Edifecs Transaction Management through 2021-07-12, an unauthenticated user can inject arbitrary text into a user's browser via logon.jsp?logon_error= on the login screen of the Web application. **CVE ID : CVE-2021-36381**	https://www.edifecs.com/services/managed-services/	A-EDI-TRAN-200721/84
emarketdegisn					
request_a_quote					
Improper	12-Jul-21	3.5	The Request a Quote	https://wpsc	A-EMA-REQU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			WordPress plugin before 2.3.4 did not sanitise and escape some of its quote fields when adding/editing a quote as admin, leading to Stored Cross-Site scripting issues when the quote is output in the 'All Quotes" table. **CVE ID : CVE-2021-24420**	an.com/vulnerability/426eafb1-0261-4e7e-8c70-75bf4c476f18	200721/85
Esri					
arcgis_server					
Server-Side Request Forgery (SSRF)	11-Jul-21	6.4	A Server-Side Request Forgery (SSRF) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote, unauthenticated attacker to forge GET requests to arbitrary URLs from the system, potentially leading to network enumeration or facilitating other attacks. **CVE ID : CVE-2021-29102**	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-server-security-2021-update-1-patch/	A-ESR-ARCG-200721/86
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-21	4.3	A reflected Cross Site Scripting (XXS) vulnerability in ArcGIS Server version 10.8.1 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser. **CVE ID : CVE-2021-29103**	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-server-security-2021-update-1-patch/	A-ESR-ARCG-200721/87
Improper	11-Jul-21	4.3	A stored Cross Site Scripting	https://ww	A-ESR-ARCG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			(XXS) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application. **CVE ID : CVE-2021-29104**	w.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-server-security-2021-update-1-patch/	200721/88
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Jul-21	3.5	A stored Cross Site Scripting (XSS) vulnerability in Esri ArcGIS Server Services Directory version 10.8.1 and below may allow a remote authenticated attacker to pass and store malicious strings in the ArcGIS Services Directory. **CVE ID : CVE-2021-29105**	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-server-security-2021-update-1-patch/	A-ESR-ARCG-200721/89
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jul-21	4.3	A reflected Cross Site Scripting (XSS) vulnerability in Esri ArcGIS Server version 10.8.1 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser. **CVE ID : CVE-2021-29106**	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-server-security-2021-update-1-patch/	A-ESR-ARCG-200721/90
Improper Neutralizatio	10-Jul-21	4.3	A stored Cross Site Scripting (XXS) vulnerability in ArcGIS	https://www.esri.com/a	A-ESR-ARCG-200721/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			Server Manager version 10.8.1 and below may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application. **CVE ID : CVE-2021-29107**	rcgis-blog/products/arcgis-enterprise/administration/arcgis-server-security-2021-update-1-patch/	
export_users_with_meta_project					
export_users_with_meta					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jul-21	6.5	The Export Users With Meta WordPress plugin before 0.6.5 did not escape the list of roles to export before using them in a SQL statement in the export functionality, available to admins, leading to an authenticated SQL Injection. **CVE ID : CVE-2021-24451**	https://wpscan.com/vulnerability/40603382-404b-44a2-8212-f2008366891c	A-EXP-EXPO-200721/92
eyecix					
jobsearch_wp_job_board					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	3.5	The WP JobSearch WordPress plugin before 1.7.4 did not sanitise or escape multiple of its parameters from the my-resume page before outputting them in the page, allowing low privilege users to use JavaScript payloads in them and leading to a Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24421**	https://wpscan.com/vulnerability/b378d36d-66d9-4373-a628-e379e4766375	A-EYE-JOBS-200721/93
fetchdesigns					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sign-up_sheets					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	3.5	The Sign-up Sheets WordPress plugin before 1.0.14 did not sanitise or escape some of its fields when creating a new sheet, allowing high privilege users to add JavaScript in them, leading to a Stored Cross-Site Scripting issue. The payloads will be triggered when viewing the 'All Sheets' page in the admin dashboard **CVE ID : CVE-2021-24440**	https://wpscan.com/vulnerability/ba4503f7-684e-4274-bc53-3aa848712496	A-FET-SIGN-200721/94
Improper Neutralization of Formula Elements in a CSV File	12-Jul-21	6	The Sign-up Sheets WordPress plugin before 1.0.14 does not not sanitise or validate the Sheet title when generating the CSV to export, which could lead to a CSV injection issue **CVE ID : CVE-2021-24441**	https://wpscan.com/vulnerability/ec9292b1-5cbd-4332-bdb6-2351c94f5ac6	A-FET-SIGN-200721/95
flask-user_project					
flask-user					
URL Redirection to Untrusted Site ('Open Redirect')	05-Jul-21	5.8	This affects all versions of package Flask-User. When using the make_safe_url function, it is possible to bypass URL validation and redirect a user to an arbitrary URL by providing multiple back slashes such as /////evil.com/path or \\\\evil.com/path. This vulnerability is only exploitable if an alternative WSGI server other than Werkzeug is used, or the default behaviour of	N/A	A-FLA-FLAS-200721/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Werkzeug is modified using 'autocorrect_location_header =False. **CVE ID : CVE-2021-23401**		
flowdroid_project					
flowdroid					
Improper Restriction of XML External Entity Reference	12-Jul-21	3.5	FlowDroid is a data flow analysis tool. FlowDroid versions prior to 2.9.0 contained an XML external entity (XXE) vulnerability that allowed an attacker who had control over the source/sink definition file in XML format to read files from external locations. In order for this to occur, the XML-based format for sources and sinks had to be used and the attacker had to able control the source/sink definition file. The vulnerability was patched in version 2.9.0. As a workaround, do not allow untrusted entities to control the source/sink definition file. **CVE ID : CVE-2021-32754**	https://github.com/secure-software-engineering/FlowDroid/security/advisories/GHSA-39r7-275f-rvgw	A-FLO-FLOW-200721/97
fluentforms					
contact_form					
Cross-Site Request Forgery (CSRF)	07-Jul-21	6.8	The WP Fluent Forms plugin < 3.6.67 for WordPress is vulnerable to Cross-Site Request Forgery leading to stored Cross-Site Scripting and limited Privilege Escalation due to a missing	https://plugins.trac.wordpress.org/browser/fluentform/trunk/app/Modules/Acl/Acl.php	A-FLU-CONT-200721/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			nonce check in the access control function for administrative AJAX actions **CVE ID : CVE-2021-34620**	?rev=2196688	
Fork-cms					
fork_cms					
Unrestricted Upload of File with Dangerous Type	07-Jul-21	6.5	Arbitrary file upload vulnerability in Fork CMS 5.9.2 allows attackers to create or replace arbitrary files in the /themes directory via a crafted zip file uploaded to the Themes panel. **CVE ID : CVE-2021-28931**	N/A	A-FOR-FORK-200721/99
Fortinet					
fortiap					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Jul-21	4.6	An improper neutralization of special elements used in an OS Command vulnerability in FortiAP's console 6.4.1 through 6.4.5 and 6.2.4 through 6.2.5 may allow an authenticated attacker to execute unauthorized commands by running the kdbg CLI command with specifically crafted arguments. **CVE ID : CVE-2021-26106**	https://fortiguard.com/advisory/FG-IR-20-210	A-FOR-FORT-200721/100
fortiap-s					
Improper Neutralization of Special Elements used in an OS Command	09-Jul-21	4.6	An improper neutralization of special elements used in an OS Command vulnerability in FortiAP's console 6.4.1 through 6.4.5 and 6.2.4 through 6.2.5 may	https://fortiguard.com/advisory/FG-IR-20-210	A-FOR-FORT-200721/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			allow an authenticated attacker to execute unauthorized commands by running the kdbg CLI command with specifically crafted arguments. **CVE ID : CVE-2021-26106**		
fortiap-w2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Jul-21	4.6	An improper neutralization of special elements used in an OS Command vulnerability in FortiAP's console 6.4.1 through 6.4.5 and 6.2.4 through 6.2.5 may allow an authenticated attacker to execute unauthorized commands by running the kdbg CLI command with specifically crafted arguments. **CVE ID : CVE-2021-26106**	https://fortiguard.com/advisory/FG-IR-20-210	A-FOR-FORT-200721/102
fortiauthenticator					
Use of Hard-coded Credentials	06-Jul-21	5	Usage of hard-coded cryptographic keys to encrypt configuration files and debug logs in FortiAuthenticator versions before 6.3.0 may allow an attacker with access to the files or the CLI configuration to decrypt the sensitive data, via knowledge of the hard-coded key. **CVE ID : CVE-2021-24005**	https://fortiguard.com/psirt/FG-IR-20-049	A-FOR-FORT-200721/103
forticlient					
Improper Link Resolution	12-Jul-21	7.2	An improper symlink following in FortiClient for Mac 6.4.3 and below may	https://fortiguard.com/advisory/FG-	A-FOR-FORT-200721/104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Before File Access ('Link Following')			allow an non-privileged user to execute arbitrary privileged shell commands during installation phase. **CVE ID : CVE-2021-26089**	IR-21-022	
fortimail					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Jul-21	6.5	Multiple instances of incorrect calculation of buffer size in the Webmail and Administrative interface of FortiMail before 6.4.5 may allow an authenticated attacker with regular webmail access to trigger a buffer overflow and to possibly execute unauthorized code or commands via specifically crafted HTTP requests. **CVE ID : CVE-2021-22129**	https://fortiguard.com/advisory/FG-IR-21-023	A-FOR-FORT-200721/105
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jul-21	7.5	Multiple improper neutralization of special elements of SQL commands vulnerabilities in FortiMail before 6.4.4 may allow a non-authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests. **CVE ID : CVE-2021-24007**	https://fortiguard.com/advisory/FG-IR-21-012	A-FOR-FORT-200721/106
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Jul-21	4	Multiple Path traversal vulnerabilities in the Webmail of FortiMail before 6.4.4 may allow a regular user to obtain unauthorized access to files and data via specifically crafted web requests.	https://fortiguard.com/advisory/FG-IR-21-014	A-FOR-FORT-200721/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24013		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Jul-21	6.5	An improper neutralization of special elements used in an OS Command vulnerability in the administrative interface of FortiMail before 6.4.4 may allow an authenticated attacker to execute unauthorized commands via specifically crafted HTTP requests. **CVE ID : CVE-2021-24015**	https://fortiguard.com/advisory/FG-IR-21-021	A-FOR-FORT-200721/108
Inadequate Encryption Strength	09-Jul-21	7.5	A missing cryptographic step in the implementation of the hash digest algorithm in FortiMail 6.4.0 through 6.4.4, and 6.2.0 through 6.2.7 may allow an unauthenticated attacker to tamper with signed URLs by appending further data which allows bypass of signature verification. **CVE ID : CVE-2021-24020**	https://fortiguard.com/advisory/FG-IR-21-027	A-FOR-FORT-200721/109
Missing Release of Memory after Effective Lifetime	12-Jul-21	5	A missing release of memory after its effective lifetime vulnerability in the Webmail of FortiMail 6.4.0 through 6.4.4 and 6.2.0 through 6.2.6 may allow an unauthenticated remote attacker to exhaust available memory via specifically crafted login requests. **CVE ID : CVE-2021-26090**	https://fortiguard.com/advisory/FG-IR-21-042	A-FOR-FORT-200721/110
Use of a Broken or Risky	12-Jul-21	4	Missing cryptographic steps in the Identity-Based Encryption service of	https://fortiguard.com/advisory/FG-	A-FOR-FORT-200721/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Algorithm			FortiMail before 7.0.0 may allow an attacker who comes in possession of the encrypted master keys to compromise their confidentiality by observing a few invariant properties of the ciphertext. **CVE ID : CVE-2021-26099**	IR-20-244	
Missing Encryption of Sensitive Data	09-Jul-21	5	A missing cryptographic step in the Identity-Based Encryption service of FortiMail before 7.0.0 may allow an unauthenticated attacker who intercepts the encrypted messages to manipulate them in such a way that makes the tampering and the recovery of the plaintexts possible. **CVE ID : CVE-2021-26100**	https://fortiguard.com/advisory/FG-IR-21-003	A-FOR-FORT-200721/112
Foxitsoftware					
foxit_reader					
Out-of-bounds Write	09-Jul-21	6.8	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write via a crafted /Size key in the Trailer dictionary. **CVE ID : CVE-2021-33792**	https://www.foxitsoftware.com/support/security-bulletins.html	A-FOX-FOXI-200721/113
Improper Handling of Exceptional Conditions	09-Jul-21	4.3	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 produce incorrect PDF document signatures because the certificate name, document owner, and signature author are mishandled.	https://www.foxitsoftware.com/support/security-bulletins.html	A-FOX-FOXI-200721/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-33795		
phantompdf					
Out-of-bounds Write	09-Jul-21	6.8	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write via a crafted /Size key in the Trailer dictionary. **CVE ID : CVE-2021-33792**	https://www.foxitsoftware.com/support/security-bulletins.html	A-FOX-PHAN-200721/115
Improper Handling of Exceptional Conditions	09-Jul-21	4.3	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 produce incorrect PDF document signatures because the certificate name, document owner, and signature author are mishandled. **CVE ID : CVE-2021-33795**	https://www.foxitsoftware.com/support/security-bulletins.html	A-FOX-PHAN-200721/116
getambassador					
emissary-ingress					
Improper Certificate Validation	09-Jul-21	4.3	Emissary-Ingress (formerly Ambassador API Gateway) through 1.13.9 allows attackers to bypass client certificate requirements (i.e., mTLS cert_required) on backend upstreams when more than one TLSContext is defined and at least one configuration exists that does not require client certificate authentication. The attacker must send an SNI specifying an unprotected backend and an HTTP Host header specifying a protected backend. (2.x versions are unaffected. 1.x	N/A	A-GET-EMIS-200721/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions are unaffected with certain configuration settings involving prune_unreachable_routes and a wildcard Host resource.) **CVE ID : CVE-2021-36371**		
Getkirby					
Kirby					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-21	3.5	Kirby is a content management system. In Kirby CMS versions 3.5.5 and 3.5.6, the Panel's `ListItem` component (used in the pages and files section for example) displayed HTML in page titles as it is. This could be used for cross-site scripting (XSS) attacks. Malicious authenticated Panel users can escalate their privileges if they get access to the Panel session of an admin user. Visitors without Panel access can use the attack vector if the site allows changing site data from a frontend form. Kirby 3.5.7 patches the vulnerability. As a partial workaround, site administrators can protect against attacks from visitors without Panel access by validating or sanitizing provided data from the frontend form. **CVE ID : CVE-2021-32735**	https://github.com/getkirby/kirby/security/advisories/GHSA-2f2w-349x-vrqm, https://github.com/getkirby/kirby/releases/tag/3.5.7	A-GET-KIRB-200721/118
Gitlab					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gitlab					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-21	4.3	Client-Side code injection through Feature Flag name in GitLab CE/EE starting with 11.9 allows a specially crafted feature flag name to PUT requests on behalf of other users via clicking on a link **CVE ID : CVE-2021-22223**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22223.json	A-GIT-GITL-200721/119
Cross-Site Request Forgery (CSRF)	07-Jul-21	4.3	A cross-site request forgery vulnerability in the GraphQL API in GitLab since version 13.12 and before versions 13.12.6 and 14.0.2 allowed an attacker to call mutations as the victim **CVE ID : CVE-2021-22224**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22224.json	A-GIT-GITL-200721/120
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-21	3.5	Insufficient input sanitization in markdown in GitLab version 13.11 and up allows an attacker to exploit a stored cross-site scripting vulnerability via a specially-crafted markdown **CVE ID : CVE-2021-22225**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22225.json	A-GIT-GITL-200721/121
N/A	06-Jul-21	4.9	Under certain conditions, some users were able to push to protected branches that were restricted to deploy keys in GitLab CE/EE since version 13.9 **CVE ID : CVE-2021-22226**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22226.json	A-GIT-GITL-200721/122
Improper Neutralization of Input During Web Page	07-Jul-21	4.3	A reflected cross-site script vulnerability in GitLab before versions 13.11.6, 13.12.6 and 14.0.2 allowed an attacker to send a	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-	A-GIT-GITL-200721/123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			malicious link to a victim and trigger actions on their behalf if they clicked it **CVE ID : CVE-2021-22227**	2021-22227.json	
Improper Authentication	06-Jul-21	4	An issue has been discovered in GitLab affecting all versions. Improper access control allows unauthorised users to access project details using Graphql. **CVE ID : CVE-2021-22228**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22228.json	A-GIT-GITL-200721/124
N/A	06-Jul-21	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting with 12.8. Under a special condition it was possible to access data of an internal repository through project fork done by a project member. **CVE ID : CVE-2021-22229**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22229.json	A-GIT-GITL-200721/125
N/A	07-Jul-21	6.5	Improper code rendering while rendering merge requests could be exploited to submit malicious code. This vulnerability affects GitLab CE/EE 9.3 and later through 13.11.6, 13.12.6, and 14.0.2. **CVE ID : CVE-2021-22230**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22230.json	A-GIT-GITL-200721/126
N/A	07-Jul-21	4	A denial of service in user's profile page is found starting with GitLab CE/EE 8.0 that allows attacker to reject access to their profile page via using a specially crafted username.	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22231.json	A-GIT-GITL-200721/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22231		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Jul-21	3.5	HTML injection was possible via the full name field before versions 13.11.6, 13.12.6, and 14.0.2 in GitLab CE **CVE ID : CVE-2021-22232**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22232.json	A-GIT-GITL-200721/128
Exposure of Sensitive Information to an Unauthorized Actor	07-Jul-21	4	An information disclosure vulnerability in GitLab EE versions 13.10 and later allowed a user to read project details **CVE ID : CVE-2021-22233**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22233.json	A-GIT-GITL-200721/129
GNU					
libredwg					
Double Free	01-Jul-21	6.8	GNU LibreDWG 0.12.3.4163 through 0.12.3.4191 has a double-free in bit_chain_free (called from dwg_encode_MTEXT and dwg_encode_add_object). **CVE ID : CVE-2021-36080**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=31724, https://github.com/LibreDWG/libredwg/commit/9b6e0ff9ef02818df034fc42c3bd149a5ff89342	A-GNU-LIBR-200721/130
Google					
chrome					
Use After Free	02-Jul-21	6.8	Use after free in WebGL in Google Chrome prior to 91.0.4472.114 allowed a	https://crbug.com/1219857,	A-GOO-CHRO-200721/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30554**	https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_17.html	
Use After Free	02-Jul-21	6.8	Use after free in Sharing in Google Chrome prior to 91.0.4472.114 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page and user gesture. **CVE ID : CVE-2021-30555**	https://crbug.com/1215029, https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_17.html	A-GOO-CHRO-200721/132
Use After Free	02-Jul-21	6.8	Use after free in WebAudio in Google Chrome prior to 91.0.4472.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30556**	https://crbug.com/1212599, https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_17.html	A-GOO-CHRO-200721/133
Use After Free	02-Jul-21	6.8	Use after free in TabGroups in Google Chrome prior to 91.0.4472.114 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a	https://crbug.com/1202102, https://chromereleases.googleblog.com/2021/06/	A-GOO-CHRO-200721/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTML page. **CVE ID : CVE-2021-30557**	stable-channel-update-for-desktop_17.html	
gu-global					
gu					
Incorrect Authorization	07-Jul-21	4.3	Improper authorization in handler for custom URL scheme vulnerability in GU App for Android versions from 4.8.0 to 5.0.2 allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App. **CVE ID : CVE-2021-20777**	N/A	A-GU--GU-200721/135
gvectors					
wpforo_forum					
URL Redirection to Untrusted Site ('Open Redirect')	06-Jul-21	5.8	The wpForo Forum WordPress plugin before 1.9.7 did not validate the redirect_to parameter in the login form of the forum, leading to an open redirect issue after a successful login. Such issue could allow an attacker to induce a user to use a login URL redirecting to a website under their control and being a replica of the legitimate one, asking them to re-enter their credentials (which will then in the attacker hands) **CVE ID : CVE-2021-24406**	https://wpscan.com/vulnerability/a9284931-555b-4c96-86a3-09e1040b0388	A-GVE-WPFO-200721/136
hms-networks					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ecatcher					
Incorrect Default Permissions	09-Jul-21	6.8	In HMS Ewon eCatcher through 6.6.4, weak filesystem permissions could allow malicious users to access files that could lead to sensitive information disclosure, modification of configuration files, or disruption of normal system operation. **CVE ID : CVE-2021-33214**	https://www.ewon.biz/technical-support/pages/talk2m/talk2m-tools/talk2m-ecatcher, https://cdn.hms-networks.com/docs/librariesprovider6/cybersecurity/hms-security-advisory-2021-07-09-001---ewon-ecatcher.pdf?sfvrsn=b37418d7_4	A-HMS-ECAT-200721/137
IBM					
app_connect_enterprise_certified_container					
Insertion of Sensitive Information into Log File	07-Jul-21	2.1	IBM App Connect Enterprise Certified Container 1.0, 1.1, 1.2, and 1.3 could allow a privileged user to obtain sensitive information from internal log files. IBM X-Force ID: 202212. **CVE ID : CVE-2021-29759**	https://exchange.xforce.ibmcloud.com/vulnerabilities/202212, https://www.ibm.com/support/pages/node/6469449	A-IBM-APP_-200721/138
cloud_pak_for_applications					
Inadequate Encryption Strength	13-Jul-21	5	IBM Cloud Pak for Applications 4.3 uses weaker than expected cryptographic	https://www.ibm.com/support/page	A-IBM-CLOU-200721/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195031. **CVE ID : CVE-2021-20360**	s/node/6471271	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jul-21	3.5	IBM Cloud Pak for Applications 4.3 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: 195032. **CVE ID : CVE-2021-20361**	https://www.ibm.com/support/pages/node/6471269	A-IBM-CLOU-200721/140
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jul-21	3.5	IBM Cloud Pak for Applications 4.3 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: 195033. **CVE ID : CVE-2021-20362**	https://www.ibm.com/support/pages/node/6471343	A-IBM-CLOU-200721/141
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jul-21	3.5	IBM Cloud Pak for Applications 4.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality	https://www.ibm.com/support/pages/node/6471341	A-IBM-CLOU-200721/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195034. **CVE ID : CVE-2021-20363**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jul-21	3.5	IBM Cloud Pak for Applications 4.3 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: 195035. **CVE ID : CVE-2021-20364**	https://www.ibm.com/support/pages/node/6471339	A-IBM-CLOU-200721/143
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jul-21	3.5	IBM Cloud Pak for Applications 4.3 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: 195036. **CVE ID : CVE-2021-20365**	https://www.ibm.com/support/pages/node/6471345	A-IBM-CLOU-200721/144
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jul-21	3.5	IBM Cloud Pak for Applications 4.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality	https://www.ibm.com/support/pages/node/6471337	A-IBM-CLOU-200721/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195037. **CVE ID : CVE-2021-20366**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jul-21	3.5	IBM Cloud Pak for Applications 4.3 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: 195357. **CVE ID : CVE-2021-20368**	https://www.ibm.com/support/pages/node/6471335	A-IBM-CLOU-200721/146
Inadequate Encryption Strength	13-Jul-21	4.3	IBM Cloud Pak for Applications 4.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195361. **CVE ID : CVE-2021-20369**	https://www.ibm.com/support/pages/node/6471331	A-IBM-CLOU-200721/147
Exposure of Sensitive Information to an Unauthorized Actor	13-Jul-21	5	IBM Cloud Pak for Applications 4.3 could disclose sensitive information to a malicious attacker by accessing data stored in memory. IBM X-Force ID: 196304. **CVE ID : CVE-2021-20422**	https://www.ibm.com/support/pages/node/6471327	A-IBM-CLOU-200721/148
Incorrect Permission Assignment for Critical	13-Jul-21	6.5	IBM Cloud Pak for Applications 4.3 could allow an authenticated user gain escalated privilesges due to improper application	https://www.ibm.com/support/pages/node/6471	A-IBM-CLOU-200721/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			permissions. IBM X-Force ID: 196308. **CVE ID : CVE-2021-20423**	329	
Generation of Error Message Containing Sensitive Information	13-Jul-21	4	IBM Cloud Pak for Applications 4.3 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. X-Force ID: 196309. **CVE ID : CVE-2021-20424**	https://www.ibm.com/support/pages/node/6471325	A-IBM-CLOU-200721/150
event_streams					
Improper Privilege Management	12-Jul-21	6.5	IBM Event Streams 10.0, 10.1, 10.2, and 10.3 could allow a user the CA private key to create their own certificates and deploy them in the cluster and gain privileges of another user. IBM X-Force ID: 203450. **CVE ID : CVE-2021-29792**	https://www.ibm.com/support/pages/node/6469451, https://exchange.xforce.ibmcloud.com/vulnerabilities/203450	A-IBM-EVEN-200721/151
guardium_data_encryption					
Insufficient Session Expiration	07-Jul-21	6.5	IBM Guardium Data Encryption (GDE) 3.0.0.2 and 4.0.0.4 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 195709. **CVE ID : CVE-2021-20378**	https://www.ibm.com/support/pages/node/6469407, https://exchange.xforce.ibmcloud.com/vulnerabilities/195709	A-IBM-GUAR-200721/152
Use of a Broken or	07-Jul-21	5	IBM Guardium Data Encryption (GDE) 3.0.0.3	https://www.ibm.com/s	A-IBM-GUAR-200721/153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Risky Cryptographic Algorithm			and 4.0.0.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195711. **CVE ID : CVE-2021-20379**	upport/pages/node/6469407, https://exchange.xforce.ibmcloud.com/vulnerabilities/195711	
N/A	12-Jul-21	4	IBM Guardium Data Encryption (GDE) 3.0.0.2 could allow a user to bruce force sensitive information due to not properly limiting the number of interactions. IBM X-Force ID: 196216. **CVE ID : CVE-2021-20414**	https://www.ibm.com/support/pages/node/6470849, https://exchange.xforce.ibmcloud.com/vulnerabilities/196216	A-IBM-GUAR-200721/154
Insufficiently Protected Credentials	07-Jul-21	5	IBM Guardium Data Encryption (GDE) 4.0.0.4 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 196217. **CVE ID : CVE-2021-20415**	https://www.ibm.com/support/pages/node/6469691, https://exchange.xforce.ibmcloud.com/vulnerabilities/196217	A-IBM-GUAR-200721/155
Exposure of Resource to Wrong Sphere	07-Jul-21	5	IBM Guardium Data Encryption (GDE) 3.0.0.3 and 4.0.0.4 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 196218.	https://www.ibm.com/support/pages/node/6469407, https://exchange.xforce.ibmcloud.com/vulnerabilities/196218	A-IBM-GUAR-200721/156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20416		
Generation of Error Message Containing Sensitive Information	07-Jul-21	4	IBM Guardium Data Encryption (GDE) 4.0.0.4 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: 196219 **CVE ID : CVE-2021-20417**	https://www.ibm.com/support/pages/node/6469691, https://exchange.xforce.ibmcloud.com/vulnerabilities/196219	A-IBM-GUAR-200721/157
Missing Authentication for Critical Function	07-Jul-21	5	IBM Guardium Data Encryption (GDE) 3.0.0.2 and 4.0.0.4 does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. **CVE ID : CVE-2021-20474**	https://www.ibm.com/support/pages/node/6469407, https://exchange.xforce.ibmcloud.com/vulnerabilities/196945	A-IBM-GUAR-200721/158
infosphere_information_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-21	4.3	IBM InfoSphere Information Server 11.7 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: 200966. **CVE ID : CVE-2021-29712**	https://www.ibm.com/support/pages/node/6468581, https://exchange.xforce.ibmcloud.com/vulnerabilities/200966	A-IBM-INFO-200721/159
Improper Neutralizatio	09-Jul-21	6.5	IBM InfoSphere Information Server 11.7 is vulnerable to	https://exchange.xforce.i	A-IBM-INFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 201164. **CVE ID : CVE-2021-29730**	bmcloud.com/vulnerabilities/201164, https://www.ibm.com/support/pages/node/6468569	200721/160
tivoli_netcool\\/impact					
Inadequate Encryption Strength	12-Jul-21	5	IBM Tivoli Netcool/Impact 7.1.0.20 and 7.1.0.21 uses an insecure SSH server configuration which enables weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 203556. **CVE ID : CVE-2021-29794**	https://exchange.xforce.ibmcloud.com/vulnerabilities/203556, https://www.ibm.com/support/pages/node/6469953	A-IBM-TIVO-200721/161
tivoli_netcool\\/omnibus_gui					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	3.5	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: 204164. **CVE ID : CVE-2021-29803**	https://www.ibm.com/support/pages/node/6471067, https://exchange.xforce.ibmcloud.com/vulnerabilities/204164	A-IBM-TIVO-200721/162
Improper Neutralizatio	12-Jul-21	3.5	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0	https://exchange.xforce.i	A-IBM-TIVO-200721/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			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: 204262. **CVE ID : CVE-2021-29804**	bmcloud.com/vulnerabilities/204262, https://www.ibm.com/support/pages/node/6471067	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	3.5	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: 204263. **CVE ID : CVE-2021-29805**	https://www.ibm.com/support/pages/node/6471067, https://exchange.xforce.ibmcloud.com/vulnerabilities/204263	A-IBM-TIVO-200721/164
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	3.5	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: 204349. **CVE ID : CVE-2021-29822**	https://www.ibm.com/support/pages/node/6471067, https://exchange.xforce.ibmcloud.com/vulnerabilities/204349	A-IBM-TIVO-200721/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
urbancode_deploy					
Incorrect Permission Assignment for Critical Resource	08-Jul-21	4	IBM UrbanCode Deploy (UCD) 6.2.7.3, 6.2.7.4, 6.2.7.8, 6.2.7.9, 7.0.3.0, 7.0.4.0, 7.0.5.4, 7.1.0.0, 7.1.1.0, 7.1.1.1, and 7.1.1.2 could allow an authenticated user with certain permissions to initiate an agent upgrade through the CLI interface. IBM X-Force ID: 200965. **CVE ID : CVE-2021-29711**	https://www.ibm.com/support/pages/node/6469941, https://exchange.xforce.ibmcloud.com/vulnerabilities/200965	A-IBM-URBA-200721/166
Icinga					
icinga					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Jul-21	3.5	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface. Between versions 2.3.0 and 2.8.2, the `doc` module of Icinga Web 2 allows to view documentation directly in the UI. It must be enabled manually by an administrator and users need explicit access permission to use it. Then, by visiting a certain route, it is possible to gain access to arbitrary files readable by the web-server user. The issue has been fixed in the 2.9.0, 2.8.3, and 2.7.5 releases. As a workaround, an administrator may disable the `doc` module or revoke permission to use it from all users. **CVE ID : CVE-2021-32746**	https://github.com/Icinga/icingaweb2/security/advisories/GHSA-cmgc-h4cx-3v43	A-ICI-ICIN-200721/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	12-Jul-21	4	Icinga Web 2 is an open source monitoring web interface, framework, and command-line interface. A vulnerability in which custom variables are exposed to unauthorized users exists between versions 2.0.0 and 2.8.2. Custom variables are user-defined keys and values on configuration objects in Icinga 2. These are commonly used to reference secrets in other configurations such as check commands to be able to authenticate with a service being checked. Icinga Web 2 displays these custom variables to logged in users with access to said hosts or services. In order to protect the secrets from being visible to anyone, it's possible to setup protection rules and blacklists in a user's role. Protection rules result in `***` being shown instead of the original value, the key will remain. Backlists will hide a custom variable entirely from the user. Besides using the UI, custom variables can also be accessed differently by using an undocumented URL parameter. By adding a parameter to the affected routes, Icinga Web 2 will show these columns	https://github.com/Icinga/icingaweb2/security/advisories/GHSA-2xv9-886q-p7xx	A-ICI-ICIN-200721/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			additionally in the respective list. This parameter is also respected when exporting to JSON or CSV. Protection rules and blacklists however have no effect in this case. Custom variables are shown as-is in the result. The issue has been fixed in the 2.9.0, 2.8.3, and 2.7.5 releases. As a workaround, one may set up a restriction to hide hosts and services with the custom variable in question. **CVE ID : CVE-2021-32747**		
ikalka_rss_reader_project					
ikalka_rss_reader					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-21	4.3	Cross-site scripting vulnerability in IkaIka RSS Reader all versions allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20752**	N/A	A-IKA-IKAL-200721/169
Iobit					
advanced_systemcare_ultimate					
Improper Privilege Management	07-Jul-21	4.6	A privilege escalation vulnerability exists in the IOCTL 0x9c406144 handling of IOBit Advanced SystemCare Ultimate 14.2.0.220. A specially crafted I/O request packet (IRP) can lead to increased privileges. An attacker can send a malicious IRP to trigger this vulnerability.	https://talosintelligence.com/vulnerability_reports/TALOS-2021-1253	A-IOB-ADVA-200721/170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21786		
N/A	07-Jul-21	4.6	A privilege escalation vulnerability exists in the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O write requests. During IOCTL 0x9c40a0d8, the first dword passed in the input buffer is the device port to write to and the byte at offset 4 is the value to write via the OUT instruction. The OUT instruction can write one byte to the given I/O device port, potentially leading to escalated privileges of unprivileged users. **CVE ID : CVE-2021-21787**	N/A	A-IOB-ADVA-200721/171
N/A	07-Jul-21	4.6	A privilege escalation vulnerability exists in the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O write requests. During IOCTL 0x9c40a0dc, the first dword passed in the input buffer is the device port to write to and the word at offset 4 is the value to write via the OUT instruction. The OUT instruction can write one byte to the given I/O device port, potentially leading to escalated privileges of unprivileged users. A local attacker can send a malicious IRP to trigger this	N/A	A-IOB-ADVA-200721/172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. **CVE ID : CVE-2021-21788**		
N/A	07-Jul-21	4.6	A privilege escalation vulnerability exists in the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O write requests. During IOCTL 0x9c40a0e0, the first dword passed in the input buffer is the device port to write to and the dword at offset 4 is the value to write via the OUT instruction. A local attacker can send a malicious IRP to trigger this vulnerability. **CVE ID : CVE-2021-21789**	N/A	A-IOB-ADVA-200721/173
irislink					
irisnext					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-21	3.5	Multiple stored XSS vulnerabilities in IrisNext Edition 9.5.16, which allows an authenticated (or compromised) user to inject malicious JavaScript in folder/file name within the application in order to grab other users' sessions or execute malicious code in their browsers (1-click RCE). **CVE ID : CVE-2021-27930**	N/A	A-IRI-IRIS-200721/174
issabel					
pbx					
Improper Neutralization of Input	06-Jul-21	3.5	A stored cross site scripting (XSS) vulnerability in index.php?menu=billing_rate	N/A	A-ISS-PBX-200721/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			s of Issabel PBX version 4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Name" or "Prefix" fields under the "Create New Rate" module. **CVE ID : CVE-2021-34190**		
izsoft					
easy_cookies_policy					
Improper Access Control	06-Jul-21	4	The Easy Cookies Policy WordPress plugin through 1.6.2 is lacking any capability and CSRF check when saving its settings, allowing any authenticated users (such as subscriber) to change them. If users can't register, this can be done through CSRF. Furthermore, the cookie banner setting is not sanitised or validated before being output in all pages of the frontend and the backend settings one, leading to a Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24405**	https://wpscan.com/vulnerability/9157d6d2-4bda-4fcd-8192-363a63a51ff5	A-IZS-EASY-200721/176
Joomla					
joomla\\!					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-21	4.3	An issue was discovered in Joomla! 3.0.0 through 3.9.27. Inadequate escaping in the rules field of the JForm API leads to a XSS vulnerability. **CVE ID : CVE-2021-26035**	https://developer.joomla.org/security-centre/856-20210701-core-xss-in-jform-rules-field.html	A-JOO-JOOM-200721/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Jul-21	5	An issue was discovered in Joomla! 2.5.0 through 3.9.27. Missing validation of input could lead to a broken usergroups table. **CVE ID : CVE-2021-26036**	https://developer.joomla.org/security-centre/857-20210702-core-dos-through-usergroup-table-manipulation.html	A-JOO-JOOM-200721/178
Insufficient Session Expiration	07-Jul-21	5	An issue was discovered in Joomla! 2.5.0 through 3.9.27. CMS functions did not properly termine existing user sessions when a user's password was changed or the user was blocked. **CVE ID : CVE-2021-26037**	https://developer.joomla.org/security-centre/858-20210703-core-lack-of-enforced-session-termination.html	A-JOO-JOOM-200721/179
Improper Check for Unusual or Exceptional Conditions	07-Jul-21	4.3	An issue was discovered in Joomla! 2.5.0 through 3.9.27. Install action in com_installer lack the required hardcoded ACL checks for superusers. A default system is not affected cause the default ACL for com_installer is limited to super users already. **CVE ID : CVE-2021-26038**	https://developer.joomla.org/security-centre/859-20210704-core-privilege-escalation-through-com-installer.html	A-JOO-JOOM-200721/180
Improper Neutralization of Input During Web Page Generation ('Cross-site	07-Jul-21	4.3	An issue was discovered in Joomla! 3.0.0 through 3.9.27. Inadequate escaping in the imagelist view of com_media leads to a XSS vulnerability. **CVE ID : CVE-2021-26039**	https://developer.joomla.org/security-centre/860-20210705-core-xss-in-com-media-imagelist.ht	A-JOO-JOOM-200721/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')				ml	
just-safe-set_project					
just-safe-set					
Improperly Controlled Modification of Dynamically-Determined Object Attributes	07-Jul-21	7.5	Prototype pollution vulnerability in 'just-safe-set' versions 1.0.0 through 2.2.1 allows an attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2021-25952**	https://github.com/angus-c/just/commit/dd57a476f4bb9d78c6f60741898dc04c71d2eb53	A-JUS-JUST-200721/182
Kaseya					
vsa					
Insufficiently Protected Credentials	09-Jul-21	7.5	Kaseya VSA before 9.5.7 allows credential disclosure, as exploited in the wild in July 2021. **CVE ID : CVE-2021-30116**	https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-2nd-2021	A-KAS-VSA-200721/183
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jul-21	6.5	SQL injection exists in Kaseya VSA before 9.5.6. **CVE ID : CVE-2021-30117**	N/A	A-KAS-VSA-200721/184
N/A	09-Jul-21	7.5	Kaseya VSA before 9.5.5 allows remote code execution. **CVE ID : CVE-2021-30118**	N/A	A-KAS-VSA-200721/185
Improper Neutralizatio	09-Jul-21	3.5	Cross Site Scripting (XSS) exists in Kaseya VSA before	N/A	A-KAS-VSA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			9.5.7. **CVE ID : CVE-2021-30119**		200721/186
Incorrect Authorizatio n	09-Jul-21	5	Kaseya VSA through 9.5.7 allows attackers to bypass the 2FA requirement. **CVE ID : CVE-2021-30120**	N/A	A-KAS-VSA-200721/187
Inclusion of Functionality from Untrusted Control Sphere	09-Jul-21	6.5	Local file inclusion exists in Kaseya VSA before 9.5.6. **CVE ID : CVE-2021-30121**	N/A	A-KAS-VSA-200721/188
Improper Restriction of XML External Entity Reference	09-Jul-21	6.5	An XML External Entity (XXE) issue exists in Kaseya VSA before 9.5.6. **CVE ID : CVE-2021-30201**	N/A	A-KAS-VSA-200721/189
KDE					
kimageformats					
Out-of-bounds Write	01-Jul-21	4.3	KDE KImageFormats 5.70.0 through 5.81.0 has a stack-based buffer overflow in XCFImageFormat::loadTileRLE. **CVE ID : CVE-2021-36083**	https://invent.kde.org/frameworks/kimageformats/commit/297ed9a2fe339bfe36916b9fce628c3242e5be0f, https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=33	A-KDE-KIMA-200721/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				742	
kramerav					
viaware					
Improper Privilege Management	12-Jul-21	7.5	KramerAV VIAWare, all tested versions, allow privilege escalation through misconfiguration of sudo. Sudoers permits running of multiple dangerous commands, including unzip, systemctl and dpkg. **CVE ID : CVE-2021-35064**	https://www.kramerav.com/us/product/viaware	A-KRA-VIAW-200721/191
kubiq					
wp_svg_images					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-21	3.5	The WP SVG images WordPress plugin before 3.4 did not sanitise the SVG files uploaded, which could allow low privilege users such as author+ to upload a malicious SVG and then perform XSS attacks by inducing another user to access the file directly. In v3.4, the plugin restricted such upload to editors and admin, with an option to also allow author to do so. The description of the plugin has also been updated with a security warning as upload of such content is intended. **CVE ID : CVE-2021-24386**	https://wpscan.com/vulnerability/e9b48b19-14cc-41ad-a029-f7f9ae236e4e	A-KUB-WP_S-200721/192
Linecorp					
line					
Improper Neutralizatio	13-Jul-21	4.3	LINE client for iOS before 10.16.3 allows cross site	N/A	A-LIN-LINE-200721/193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			script with specific header in WebView. **CVE ID : CVE-2021-36214**		
Linuxfoundation					
grpc_swift					
N/A	09-Jul-21	5	Mismanaged state in GRPCWebToHTTP2ServerCodec.swift in gRPC Swift 1.1.0 and 1.1.1 allows remote attackers to deny service by sending malformed requests. **CVE ID : CVE-2021-36153**	N/A	A-LIN-GRPC-200721/194
Uncontrolled Recursion	09-Jul-21	5	HTTP2ToRawGRPCServerCodec in gRPC Swift 1.1.1 and earlier allows remote attackers to deny service via the delivery of many small messages within a single HTTP/2 frame, leading to Uncontrolled Recursion and stack consumption. **CVE ID : CVE-2021-36154**	N/A	A-LIN-GRPC-200721/195
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Jul-21	5	LengthPrefixedMessageReader in gRPC Swift 1.1.0 and earlier allocates buffers of arbitrary length, which allows remote attackers to cause uncontrolled resource consumption and deny service. **CVE ID : CVE-2021-36155**	N/A	A-LIN-GRPC-200721/196
linuxptp_project					
linuxptp					
Improper	09-Jul-21	8	A flaw was found in the	https://bugz	A-LIN-LINU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			ptp4l program of the linuxptp package. A missing length check when forwarding a PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before 2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1. **CVE ID : CVE-2021-3570**	illa.redhat.com/show_bug.cgi?id=1966240	200721/197
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-21	5.5	A flaw was found in the ptp4l program of the linuxptp package. When ptp4l is operating on a little-endian architecture as a PTP transparent clock, a remote attacker could send a crafted one-step sync message to cause an information leak or crash. The highest threat from this vulnerability is to data confidentiality and system availability. This flaw affects linuxptp versions before 3.1.1 and before 2.0.1. **CVE ID : CVE-2021-3571**	https://bugzilla.redhat.com/show_bug.cgi?id=1966241	A-LIN-LINU-200721/198
Mediawiki					
mediawiki					
Exposure of Resource to	02-Jul-21	5	In MediaWiki before 1.31.15, 1.32.x through 1.35.x before	https://lists.wikimedia.or	A-MED-MEDI-200721/199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			1.35.3, and 1.36.x before 1.36.1, bots have certain unintended API access. When a bot account has a "sitewide block" applied, it is able to still "purge" pages through the MediaWiki Action API (which a "sitewide block" should have prevented). **CVE ID : CVE-2021-35197**	g/hyperkitty/list/mediawiki-announce@lists.wikimedia.org/thread/YR3X4L2CPSEJVSY543AWEO65TD6APXHP/, https://phabricator.wikimedia.org/T280226	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jul-21	5	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. The Special:GlobalRenameRequest page is vulnerable to infinite loops and denial of service attacks when a user's current username is beyond an arbitrary maximum configuration value (MaxNameChars). **CVE ID : CVE-2021-36125**	https://phabricator.wikimedia.org/T260865, https://gerrit.wikimedia.org/r/q/I97d8b3236b5abed8ba9a9c4d3ab5050c2e782c22	A-MED-MEDI-200721/200
N/A	02-Jul-21	7.5	An issue was discovered in the AbuseFilter extension in MediaWiki through 1.36. If the MediaWiki:Abusefilter-blocker message is invalid within the content language, the filter user falls back to the English version, but that English version could also be invalid on a wiki. This would result in a fatal error, and potentially fail to block or restrict a potentially nefarious user.	https://phabricator.wikimedia.org/T284364, https://gerrit.wikimedia.org/r/q/I9e9f44b7663e810de70fb9ac7f6760f83dd4895b	A-MED-MEDI-200721/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36126		
Insecure Storage of Sensitive Information	02-Jul-21	4	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. The Special:GlobalUserRights page provided search results which, for a suppressed MediaWiki user, were different than for any other user, thus easily disclosing suppressed accounts (which are supposed to be completely hidden). **CVE ID : CVE-2021-36127**	https://phabricator.wikimedia.org/T285190, https://gerrit.wikimedia.org/r/q/I4e4dbcad61e1d4f6fd8b038bf63d19c69081a8ec	A-MED-MEDI-200721/202
Improper Authentication	02-Jul-21	7.5	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. Autoblocks for CentralAuth-issued suppression blocks are not properly implemented. **CVE ID : CVE-2021-36128**	https://gerrit.wikimedia.org/r/q/I3e65690695313380c798b62edfda726b6e374f89, https://gerrit.wikimedia.org/r/q/I15d14c88a1e30df92c470bc191c4ee573172d4d1, https://phabricator.wikimedia.org/T281972	A-MED-MEDI-200721/203
Incorrect Permission Assignment for Critical Resource	02-Jul-21	4	An issue was discovered in the Translate extension in MediaWiki through 1.36. The Aggregategroups Action API module does not validate the parameter for aggregategroup when action=remove is set, thus	https://phabricator.wikimedia.org/T282932, https://gerrit.wikimedia.org/r/q/I3619a7e88c2e	A-MED-MEDI-200721/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowing users with the translate-manage right to silently delete various groups' metadata. **CVE ID : CVE-2021-36129**	b979babb7b027d4fdbfabc0af792	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-21	3.5	An XSS issue was discovered in the SocialProfile extension in MediaWiki through 1.36. Within several gift-related special pages, a privileged user with the awardmanage right could inject arbitrary HTML and JavaScript within various gift-related data fields. The attack could easily propagate across many pages for many users. **CVE ID : CVE-2021-36130**	https://phabricator.wikimedia.org/T281043, https://gerrit.wikimedia.org/r/q/Id915eba45497a1a0dc1c4e00818a2fd4c0ce55d3	A-MED-MEDI-200721/205
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-21	3.5	An XSS issue was discovered in the SportsTeams extension in MediaWiki through 1.36. Within several special pages, a privileged user could inject arbitrary HTML and JavaScript within various data fields. The attack could easily propagate across many pages for many users. **CVE ID : CVE-2021-36131**	https://phabricator.wikimedia.org/T281196, https://gerrit.wikimedia.org/r/q/Ic312cc9b8463c8e7c3298a661abfcff2cc2332cb	A-MED-MEDI-200721/206
Incorrect Authorization	02-Jul-21	6	An issue was discovered in the FileImporter extension in MediaWiki through 1.36. For certain relaxed configurations of the $wgFileImporterRequiredRight variable, it might not validate all appropriate user rights, thus allowing a user	https://phabricator.wikimedia.org/T280590, https://gerrit.wikimedia.org/r/q/I8ff2a67abd2c118a3469e44	A-MED-MEDI-200721/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with insufficient rights to perform operations (specifically file uploads) that they should not be allowed to perform. **CVE ID : CVE-2021-36132**	10eac2a451bfa76c3	
Microfocus					
netiq_advanced_authentication					
Incorrect Authorization	12-Jul-21	4	Multi-Factor Authentication (MFA) functionality can be bypassed, allowing the use of single factor authentication in NetIQ Advanced Authentication versions prior to 6.3 SP4 Patch 1. **CVE ID : CVE-2021-22515**	https://www.netiq.com/documentation/advanced-authentication-63/advanced-authentication-releasenotes-6341/data/advanced-authentication-releasenotes-6341.html	A-MIC-NETI-200721/208
Misp					
misp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-21	4.3	app/View/SharingGroups/view.ctp in MISP before 2.4.146 allows stored XSS in the sharing groups view. **CVE ID : CVE-2021-36212**	https://github.com/MISP/MISP/commit/01521d614cb578de75a406394b4f0426f6036ba7, https://github.com/MISP/MISP/compa	A-MIS-MISP-200721/209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				re/v2.4.145...v2.4.146	
Nextcloud					
nextcloud					
Improper Certificate Validation	12-Jul-21	5	Nextcloud Android Client is the Android client for Nextcloud. Clients using the Nextcloud end-to-end encryption feature download the public and private key via an API endpoint. In versions prior to 3.16.1, the Nextcloud Android client skipped a step that involved the client checking if a private key belonged to a previously downloaded public certificate. If the Nextcloud instance served a malicious public key, the data would be encrypted for this key and thus could be accessible to a malicious actor. The vulnerability is patched in version 3.16.1. As a workaround, do not add additional end-to-end encrypted devices to a user account. **CVE ID : CVE-2021-32727**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-5v33-r9cm-7736	A-NEX-NEXT-200721/210
nextcloud_mail					
Exposure of Sensitive Information to an Unauthorized Actor	12-Jul-21	4	Nextcloud Mail is a mail app for Nextcloud. In versions prior to 1.9.6, the Nextcloud Mail application does not, by default, render images in emails to not leak the read state. The privacy filter	https://github.com/nextcloud/mail/pull/5189, https://github.com/nextcloud/security	A-NEX-NEXT-200721/211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			failed to filter images with a `background-image` CSS attribute. Note that the images were still passed through the Nextcloud image proxy, and thus there was no IP leakage. The issue was patched in version 1.9.6 and 1.10.0. No workarounds are known to exist. **CVE ID : CVE-2021-32707**	-advisories/security/advisories/GHSA-xxp4-44xc-8crh	
nextcloud_server					
Improper Restriction of Excessive Authentication Attempts	12-Jul-21	5	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.0.11, and 21.0.3, ratelimits are not applied to OCS API responses. This affects any OCS API controller (`OCSController`) using the `@BruteForceProtection` annotation. Risk depends on the installed applications on the Nextcloud Server, but could range from bypassing authentication ratelimits or spamming other Nextcloud users. The vulnerability is patched in versions 19.0.13, 20.0.11, and 21.0.3. No workarounds aside from upgrading are known to exist. **CVE ID : CVE-2021-32678**	https://github.com/nextcloud/server/pull/27329, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-48rx-3gmf-g74j	A-NEX-NEXT-200721/212
Improper Encoding or Escaping of	12-Jul-21	6.8	Nextcloud Server is a Nextcloud package that handles data storage. In	https://github.com/nextcloud/security	A-NEX-NEXT-200721/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output			versions prior to 19.0.13, 20.0.11, and 21.0.3, filenames where not escaped by default in controllers using `DownloadResponse`. When a user-supplied filename was passed unsanitized into a `DownloadResponse`, this could be used to trick users into downloading malicious files with a benign file extension. This would show in UI behaviours where Nextcloud applications would display a benign file extension (e.g. JPEG), but the file will actually be downloaded with an executable file extension. The vulnerability is patched in versions 19.0.13, 20.0.11, and 21.0.3. Administrators of Nextcloud instances do not have a workaround available, but developers of Nextcloud apps may manually escape the file name before passing it into `DownloadResponse`. **CVE ID : CVE-2021-32679**	- advisories/security/advisories/GHSA-3hjp-26x8-mhf6, https://github.com/nextcloud/server/pull/27354	
N/A	12-Jul-21	2.1	Nextcloud Server is a Nextcloud package that handles data storage. In versions priot to 19.0.13, 20.0.11, and 21.0.3, Nextcloud Server audit logging functionality wasn't properly logging events for the unsetting of a share	https://github.com/nextcloud/security - advisories/security/advisories/GHSA-fxpq-wq7c-vppf,	A-NEX-NEXT-200721/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			expiration date. This event is supposed to be logged. This issue is patched in versions 19.0.13, 20.0.11, and 21.0.3. **CVE ID : CVE-2021-32680**	https://github.com/nextcloud/server/pull/27024	
Files or Directories Accessible to External Parties	12-Jul-21	7.5	Nextcloud Server is a Nextcloud package that handles data storage. Nextcloud Server supports application specific tokens for authentication purposes. These tokens are supposed to be granted to a specific applications (e.g. DAV sync clients), and can also be configured by the user to not have any filesystem access. Due to a lacking permission check, the tokens were able to change their own permissions in versions prior to 19.0.13, 20.0.11, and 21.0.3. Thus fileystem limited tokens were able to grant themselves access to the filesystem. The issue is patched in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds aside from upgrading. **CVE ID : CVE-2021-32688**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-48m7-7r2r-838r, https://github.com/nextcloud/server/pull/27000	A-NEX-NEXT-200721/215
Improper Restriction of Excessive Authentication Attempts	12-Jul-21	5	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the shareinfo endpoint. This may have allowed an attacker to enumerate	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-375p-cxxq-gc9p,	A-NEX-NEXT-200721/216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially valid share tokens. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds. **CVE ID : CVE-2021-32703**	https://github.com/nextcloud/server/pull/26945	
Improper Restriction of Excessive Authentication Attempts	12-Jul-21	5	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the public DAV endpoint. This may have allowed an attacker to enumerate potentially valid share tokens or credentials. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds. **CVE ID : CVE-2021-32705**	https://github.com/nextcloud/server/pull/27610, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-fjv7-283f-5m54	A-NEX-NEXT-200721/217
Incorrect Default Permissions	12-Jul-21	5	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, default share permissions were not being respected for federated reshares of files and folders. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds. **CVE ID : CVE-2021-32725**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-6f6v-h9x9-jj4v, https://github.com/nextcloud/server/pull/26946	A-NEX-NEXT-200721/218
Exposure of Resource to Wrong Sphere	12-Jul-21	7.5	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13,	https://github.com/nextcloud/security-	A-NEX-NEXT-200721/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.011, and 21.0.3, webauthn tokens were not deleted after a user has been deleted. If a victim reused an earlier used username, the previous user could gain access to their account. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds. **CVE ID : CVE-2021-32726**	advisories/security/advisories/GHSA-6qr9-c846-j8mg	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	4.3	Nextcloud Text is a collaborative document editing application that uses Markdown. A cross-site scripting vulnerability is present in versions prior to 19.0.13, 20.0.11, and 21.0.3. The Nextcloud Text application shipped with Nextcloud server used a `text/html` Content-Type when serving files to users. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. As a workaround, use a browser that has support for Content-Security-Policy. **CVE ID : CVE-2021-32733**	https://github.com/nextcloud/text/pull/1689, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-x4w3-jhcr-57pq	A-NEX-NEXT-200721/220
Generation of Error Message Containing	12-Jul-21	5	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13,	https://github.com/nextcloud/security-	A-NEX-NEXT-200721/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			20.011, and 21.0.3, the Nextcloud Text application shipped with Nextcloud Server returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. As a workaround, one may disable the Nextcloud Text application in Nextcloud Server app settings. **CVE ID : CVE-2021-32734**	advisories/security/advisories/GHSA-6hf5-c2c4-2526, https://github.com/nextcloud/text/pull/1695	
N/A	12-Jul-21	5	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the public share link mount endpoint. This may have allowed an attacker to enumerate potentially valid share tokens. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds. **CVE ID : CVE-2021-32741**	https://github.com/nextcloud/server/pull/26958, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-crvj-vmf7-xrvr	A-NEX-NEXT-200721/222
talk					
Exposure of Sensitive Information to an Unauthorized Actor	12-Jul-21	4	Nextcloud Talk is a fully on-premises audio/video and chat communication service. In versions prior to 11.2.2, if a user was able to reuse an earlier used username, they could get access to any chat message sent to the previous	https://github.com/nextcloud/spreed/pull/5633, https://github.com/nextcloud/security-	A-NEX-TALK-200721/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user with this username. The issue was patched in versions 11.2.2 and 11.3.0. As a workaround, don't allow users to choose usernames themselves. This is the default behaviour of Nextcloud, but some user providers may allow doing so. **CVE ID : CVE-2021-32689**	advisories/security/advisories/GHSA-xv6f-344w-895c	
nica					
winwaste.net					
Incorrect Authorization	08-Jul-21	4.6	WinWaste.NET version 1.0.6183.16475 has incorrect permissions, allowing a local unprivileged user to replace the executable with a malicious file that will be executed with "LocalSystem" privileges. **CVE ID : CVE-2021-34110**	http://nica.it	A-NIC-WINW-200721/224
ninjarmm					
ninjarmm					
Incorrect Authorization	07-Jul-21	4.6	The Agent in NinjaRMM 5.0.909 has Incorrect Access Control. **CVE ID : CVE-2021-26273**	https://www.ninjarmm.com/blog/cve-2021-26273-cve-2021-26274/, https://www.ninjarmm.com	A-NIN-NINJ-200721/225
Incorrect Default Permissions	07-Jul-21	3.6	The Agent in NinjaRMM 5.0.909 has Insecure Permissions.	https://www.ninjarmm.com/blog/cv	A-NIN-NINJ-200721/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26274	e-2021-26273-cve-2021-26274/, https://www.ninjarmm.com	
ninjateam					
filebird					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Jul-21	7.5	The Filebird Plugin 4.7.3 introduced a SQL injection vulnerability as it is making SQL queries without escaping user input data from a HTTP post request. This is a major vulnerability as the user input is not escaped and passed directly to the get_col function and it allows SQL injection. The Rest API endpoint which invokes this function also does not have any required permissions/authentication and can be accessed by an anonymous user. **CVE ID : CVE-2021-24385**	https://wpscan.com/vulnerability/754ac750-0262-4f65-b23e-d5523995fbfa	A-NIN-FILE-200721/227
Nodejs					
node.js					
Out-of-bounds Read	12-Jul-21	6.4	Node.js before 16.4.1, 14.17.2, 12.22.2 is vulnerable to an out-of-bounds read when uv__idna_toascii() is used to convert strings to ASCII. The pointer p is read and increased without checking whether it is beyond pe, with the latter holding a pointer	https://nodejs.org/en/blog/vulnerability/july-2021-security-releases/	A-NOD-NODE-200721/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the end of the buffer. This can lead to information disclosures or crashes. This function can be triggered via uv_getaddrinfo(). **CVE ID : CVE-2021-22918**		
Incorrect Permission Assignment for Critical Resource	12-Jul-21	4.4	Node.js before 16.4.1, 14.17.2, and 12.22.2 is vulnerable to local privilege escalation attacks under certain conditions on Windows platforms. More specifically, improper configuration of permissions in the installation directory allows an attacker to perform two different escalation attacks: PATH and DLL hijacking. **CVE ID : CVE-2021-22921**	https://nodejs.org/en/blog/vulnerability/july-2021-security-releases/	A-NOD-NODE-200721/229
NSA					
emissary					
Server-Side Request Forgery (SSRF)	02-Jul-21	6.5	Emissary is a P2P-based, data-driven workflow engine. Emissary version 6.4.0 is vulnerable to Server-Side Request Forgery (SSRF). In particular, the `RegisterPeerAction` endpoint and the `AddChildDirectoryAction` endpoint are vulnerable to SSRF. This vulnerability may lead to credential leaks. Emissary version 7.0 contains a patch. As a workaround, disable network access to Emissary from untrusted sources.	https://github.com/NationalSecurityAgency/emissary/security/advisories/GHSA-2p8j-2rf3-h4xr	A-NSA-EMIS-200721/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-32639		
Ntop					
ndpi					
Out-of-bounds Write	01-Jul-21	6.8	ntop nDPI 3.4 has a stack-based buffer overflow in processClientServerHello. **CVE ID : CVE-2021-36082**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=30393, https://github.com/ntop/nDPI/commit/1ec621c85b9411cc611652fd57a892cfef478af3	A-NTO-NDPI-200721/231
octopus					
server					
Cleartext Storage of Sensitive Information	08-Jul-21	5	When configuring Octopus Server if it is configured with an external SQL database, on initial configuration the database password is written to the OctopusServer.txt log file in plaintext. **CVE ID : CVE-2021-31816**	https://advisories.octopus.com/adv/2021-05---Cleartext-Storage-of-Sensitive-Information-(CVE-2021-31816).2121793537.html	A-OCT-SERV-200721/232
Cleartext Storage of Sensitive Information	08-Jul-21	5	When configuring Octopus Server if it is configured with an external SQL database, on initial configuration the database password is written to the OctopusServer.txt log file in plaintext. **CVE ID : CVE-2021-31817**	https://advisories.octopus.com/adv/2021-06---Cleartext-Storage-of-Sensitive-Information-(CVE-2021-31817).2121	A-OCT-SERV-200721/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				138201.html	
Openexr					
openexr					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Jul-21	2.1	There's a flaw in OpenEXR's ImfDeepScanLineInputFile functionality in versions prior to 3.0.5. An attacker who is able to submit a crafted file to an application linked with OpenEXR could cause an out-of-bounds read. The greatest risk from this flaw is to application availability. **CVE ID : CVE-2021-3598**	https://bugzilla.redhat.com/show_bug.cgi?id=1970987	A-OPE-OPEN-200721/234
openthread					
wpantund					
Out-of-bounds Write	02-Jul-21	4.6	OpenThread wpantund through 2021-07-02 has a stack-based Buffer Overflow because of an inconsistency in the integer data type for metric_len. **CVE ID : CVE-2021-33889**	https://github.com/fireeye/Vulnerability-Disclosures/blob/master/FEYE-2021-0019/FEYE-2021-0019.md, https://github.com/openthread/wpantund/issues/502	A-OPE-WPAN-200721/235
Openvpn					
connect					
Uncontrolled Search Path Element	02-Jul-21	4.4	OpenVPN Connect 3.2.0 through 3.3.0 allows local users to load arbitrary dynamic loadable libraries	https://openvpn.net/vpn-server-resources/op	A-OPE-CONN-200721/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via an OpenSSL configuration file if present, which allows the user to run arbitrary code with the same privilege level as the main OpenVPN process (OpenVPNConnect.exe). **CVE ID : CVE-2021-3613**	envpn-connect-for-windows-change-log/	
openvpn					
Improper Authentication	12-Jul-21	5.8	OpenVPN 3 Core Library version 3.6 and 3.6.1 allows a man-in-the-middle attacker to bypass the certificate authentication by issuing an unrelated server certificate using the same hostname found in the verify-x509-name option in a client configuration. **CVE ID : CVE-2021-3547**	https://community.openvpn.net/openvpn/wiki/SecurityAnnouncements, https://community.openvpn.net/openvpn/wiki/CVE-2021-3547	A-OPE-OPEN-200721/237
Uncontrolled Search Path Element	02-Jul-21	4.4	OpenVPN before version 2.5.3 on Windows allows local users to load arbitrary dynamic loadable libraries via an OpenSSL configuration file if present, which allows the user to run arbitrary code with the same privilege level as the main OpenVPN process (openvpn.exe). **CVE ID : CVE-2021-3606**	https://community.openvpn.net/openvpn/wiki/SecurityAnnouncements, https://community.openvpn.net/openvpn/wiki/CVE-2021-3606	A-OPE-OPEN-200721/238
Panasonic					
fpwin_pro					
Improper Restriction of XML	09-Jul-21	4.3	Panasonic FPWIN Pro, all Versions 7.5.1.1 and prior, allows an attacker to craft a	N/A	A-PAN-FPWI-200721/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
External Entity Reference			project file specifying a URI that causes the XML parser to access the URI and embed the contents, which may allow the attacker to disclose information that is accessible in the context of the user executing software. **CVE ID : CVE-2021-32972**		
Pexip					
pexip_infinity					
Improper Input Validation	07-Jul-21	5	Pexip Infinity 25.x before 25.4 has Improper Input Validation, and thus an unauthenticated remote attacker can cause a denial of service via the administrative web interface. **CVE ID : CVE-2021-31925**	https://docs.pexip.com/admin/security_bulletins.htm, https://docs.pexip.com/admin/security_bulletins.htm#CVE-2021-31925	A-PEX-PEXI-200721/240
phone_shop_sales_managements_system_project					
phone_shop_sales_managements_system					
Use of Incorrectly-Resolved Name or Reference	01-Jul-21	4	Sourcecodester Phone Shop Sales Managements System 1.0 is vulnerable to Insecure Direct Object Reference (IDOR). Any attacker will be able to see the invoices of different users by changing the id parameter. **CVE ID : CVE-2021-35337**	N/A	A-PHO-PHON-200721/241
plugin-planet					
prismatic					
Improper Neutralizatio	12-Jul-21	3.5	The Prismatic WordPress plugin before 2.8 does not	https://wpscan.com/vuln	A-PLU-PRIS-200721/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			sanitise or validate some of its shortcode parameters, allowing users with a role as low as Contributor to set Cross-Site payload in them. A post made by a contributor would still have to be approved by an admin to have the XSS trigger able in the frontend, however, higher privilege users, such as editor could exploit this without the need of approval, and even when the blog disallows the unfiltered_html capability. **CVE ID : CVE-2021-24408**	erability/51855853-e7bd-425f-802c-824209f4f84d	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	4.3	The Prismatic WordPress plugin before 2.8 does not escape the 'tab' GET parameter before outputting it back in an attribute, leading to a reflected Cross-Site Scripting issue which will be executed in the context of a logged in administrator **CVE ID : CVE-2021-24409**	https://wpscan.com/vulnerability/ae3cd3ed-aecd-4d8c-8a2b-2936aaaef0cf	A-PLU-PRIS-200721/243
pluginus					
wordpress_meta_data_and_taxonomies_filter					
Cross-Site Request Forgery (CSRF)	14-Jul-21	6.8	Cross-site request forgery (CSRF) vulnerability in WordPress Meta Data Filter & Taxonomies Filter versions prior to v.1.2.8 and versions prior to v.2.2.8 allows remote attackers to hijack the authentication of administrators via	https://wp-filter.com/update-v-2-2-8-v-1-2-8/, https://wp-filter.com/	A-PLU-WORD-200721/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unspecified vectors. **CVE ID : CVE-2021-20781**		
profilepress					
wp-user-avatar					
Improper Privilege Management	07-Jul-21	7.5	A vulnerability in the user registration component found in the ~/src/Classes/RegistrationAuth.php file of the ProfilePress WordPress plugin made it possible for users to register on sites as an administrator. This issue affects versions 3.0.0 - 3.1.3. . **CVE ID : CVE-2021-34621**	N/A	A-PRO-WP-U-200721/245
Improper Privilege Management	07-Jul-21	6.5	A vulnerability in the user profile update component found in the ~/src/Classes/EditUserProfile.php file of the ProfilePress WordPress plugin made it possible for users to escalate their privileges to that of an administrator while editing their profile. This issue affects versions 3.0.0 - 3.1.3. . **CVE ID : CVE-2021-34622**	N/A	A-PRO-WP-U-200721/246
Unrestricted Upload of File with Dangerous Type	07-Jul-21	7.5	A vulnerability in the image uploader component found in the ~/src/Classes/ImageUploader.php file of the ProfilePress WordPress plugin made it possible for users to upload arbitrary files during user registration or during profile updates. This issue affects versions 3.0.0 - 3.1.3. .	N/A	A-PRO-WP-U-200721/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34623		
Unrestricted Upload of File with Dangerous Type	07-Jul-21	7.5	A vulnerability in the file uploader component found in the ~/src/Classes/FileUploader.php file of the ProfilePress WordPress plugin made it possible for users to upload arbitrary files during user registration or during profile updates. This issue affects versions 3.0.0 - 3.1.3. . **CVE ID : CVE-2021-34624**	N/A	A-PRO-WP-U-200721/248
Prothemedesign					
browser_screenshots					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	3.5	The Browser Screenshots WordPress plugin before 1.7.6 allowed authenticated users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks as the image_class parameter of the browser-shot shortcode was not escaped. **CVE ID : CVE-2021-24439**	https://wpscan.com/vulnerability/9c538c51-ae58-461d-b93b-cc9dfebf2bc0	A-PRO-BROW-200721/249
putil-merge_project					
putil-merge					
N/A	14-Jul-21	7.5	Prototype pollution vulnerability in 'putil-merge' versions1.0.0 through 3.6.6 allows attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2021-25953**	N/A	A-PUT-PUTI-200721/250
Putty					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
putty					
Insufficient Verification of Data Authenticity	09-Jul-21	5.8	PuTTY through 0.75 proceeds with establishing an SSH session even if it has never sent a substantive authentication response. This makes it easier for an attacker-controlled SSH server to present a later spoofed authentication prompt (that the attacker can use to capture credential data, and use that data for purposes that are undesired by the client user). **CVE ID : CVE-2021-36367**	https://git.tartarus.org/?p=simon/putty.git;a=commit;h=1dc5659aa62848f0aeb5de7bd3839fecc7debefa	A-PUT-PUTT-200721/251
pywin32_project					
pywin32					
Integer Overflow or Wraparound	06-Jul-21	4	An integer overflow exists in pywin32 prior to version b301 when adding an access control entry (ACE) to an access control list (ACL) that would cause the size to be greater than 65535 bytes. An attacker who successfully exploited this vulnerability could crash the vulnerable process. **CVE ID : CVE-2021-32559**	N/A	A-PYW-PYWI-200721/252
Qnap					
hybrid_backup_sync					
Improper Access Control	08-Jul-21	10	An improper access control vulnerability has been reported to affect certain legacy versions of HBS 3. If exploited, this vulnerability allows attackers to	https://www.qnap.com/en/security-advisory/qsa-21-19	A-QNA-HYBR-200721/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromise the security of the operating system.QNAP have already fixed this vulnerability in the following versions of HBS 3: QTS 4.3.6: HBS 3 v3.0.210507 and later QTS 4.3.4: HBS 3 v3.0.210506 and later QTS 4.3.3: HBS 3 v3.0.210506 and later **CVE ID : CVE-2021-28809**		
q\\"center					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jul-21	3.5	This issue affects: QNAP Systems Inc. Q'center versions prior to 1.11.1004. **CVE ID : CVE-2021-28803**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-31	A-QNA-Q\\'-200721/254
qsan					
sanos					
Use of Password Hash With Insufficient Computational Effort	07-Jul-21	5	Use of password hash with insufficient computational effort vulnerability in QSAN Storage Manager, XEVO, SANOS allows remote attackers to recover the plain-text password by brute-forcing the MD5 hash. **CVE ID : CVE-2021-32519**	https://www.twcert.org.tw/tw/cp-132-4875-692f0-1.html	A-QSA-SANO-200721/255
Use of Hard-coded Credentials	07-Jul-21	7.5	Use of MAC address as an authenticated password in QSAN Storage Manager, XEVO, SANOS allows local attackers to escalate privileges. **CVE ID : CVE-2021-32521**	https://www.twcert.org.tw/tw/cp-132-4877-7b696-1.html	A-QSA-SANO-200721/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	07-Jul-21	5	Improper restriction of excessive authentication attempts vulnerability in QSAN Storage Manager, XEVO, SANOS allows remote attackers to discover users' credentials and obtain access via a brute force attack. **CVE ID : CVE-2021-32522**	https://www.twcert.org.tw/tw/cp-132-4878-0a279-1.html	A-QSA-SANO-200721/257
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Jul-21	7.5	Command injection vulnerability in QSAN XEVO, SANOS allows remote unauthenticated attackers to execute arbitrary commands. **CVE ID : CVE-2021-32529**	https://www.twcert.org.tw/tw/cp-132-4885-b03c8-1.html	A-QSA-SANO-200721/258
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	7.5	The QSAN SANOS setting page does not filter special parameters. Remote attackers can use this vulnerability to inject and execute arbitrary commands without permissions. **CVE ID : CVE-2021-32533**	https://www.twcert.org.tw/tw/cp-132-4890-39791-1.html	A-QSA-SANO-200721/259
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	7.5	QSAN SANOS factory reset function does not filter special parameters. Remote attackers can use this vulnerability to inject and execute arbitrary commands without permissions. **CVE ID : CVE-2021-32534**	https://www.twcert.org.tw/tw/cp-132-4891-94707-1.html	A-QSA-SANO-200721/260
Use of Hard-coded Credentials	07-Jul-21	7.5	The vulnerability of hard-coded default credentials in QSAN SANOS allows	https://www.twcert.org.tw/tw/cp-	A-QSA-SANO-200721/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attackers to obtain administrator's permission and execute arbitrary functions. **CVE ID : CVE-2021-32535**	132-4892-768d9-1.html	
storage_manager					
Absolute Path Traversal	07-Jul-21	4	Absolute Path Traversal vulnerability in GetImage in QSAN Storage Manager allows remote authenticated attackers download arbitrary files via the Url path parameter. **CVE ID : CVE-2021-32506**	https://www.twcert.org.tw/tw/cp-132-4862-f8b86-1.html	A-QSA-STOR-200721/262
Absolute Path Traversal	07-Jul-21	4	Absolute Path Traversal vulnerability in FileDownload in QSAN Storage Manager allows remote authenticated attackers download arbitrary files via the Url path parameter. **CVE ID : CVE-2021-32507**	https://www.twcert.org.tw/tw/cp-132-4863-57d4a-1.html	A-QSA-STOR-200721/263
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jul-21	4	Absolute Path Traversal vulnerability in FileStreaming in QSAN Storage Manager allows remote authenticated attackers access arbitrary files by injecting the Symbolic Link following the Url path parameter. **CVE ID : CVE-2021-32508**	https://www.twcert.org.tw/tw/cp-132-4864-94df4-1.html	A-QSA-STOR-200721/264
UNIX Symbolic Link (Symlink)	07-Jul-21	4	Absolute Path Traversal vulnerability in FileviewDoc in QSAN Storage Manager allows remote authenticated	https://www.twcert.org.tw/tw/cp-132-4865-	A-QSA-STOR-200721/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Following			attackers access arbitrary files by injecting the Symbolic Link following the Url path parameter. **CVE ID : CVE-2021-32509**	0c967-1.html	
Exposure of Information Through Directory Listing	07-Jul-21	4	QSAN Storage Manager through directory listing vulnerability in antivirus function allows remote authenticated attackers to list arbitrary directories by injecting file path parameter. **CVE ID : CVE-2021-32510**	https://www.twcert.org.tw/tw/cp-132-4866-b820b-1.html	A-QSA-STOR-200721/266
N/A	07-Jul-21	4	QSAN Storage Manager through directory listing vulnerability in ViewBroserList allows remote authenticated attackers to list arbitrary directories via the file path parameter. **CVE ID : CVE-2021-32511**	https://www.twcert.org.tw/tw/cp-132-4867-9c11c-1.html	A-QSA-STOR-200721/267
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	7.5	QuickInstall in QSAN Storage Manager does not filter special parameters properly that allows remote unauthenticated attackers to inject and execute arbitrary commands. **CVE ID : CVE-2021-32512**	https://www.twcert.org.tw/tw/cp-132-4868-75574-1.html	A-QSA-STOR-200721/268
Improper Neutralization of Special Elements used in an OS Command ('OS Command	07-Jul-21	7.5	QsanTorture in QSAN Storage Manager does not filter special parameters properly that allows remote unauthenticated attackers to inject and execute arbitrary commands.	https://www.twcert.org.tw/tw/cp-132-4869-714a5-1.html	A-QSA-STOR-200721/269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			**CVE ID : CVE-2021-32513**		
Improper Access Control	07-Jul-21	5	Improper access control vulnerability in FirmwareUpgrade in QSAN Storage Manager allows remote attackers to reboot and discontinue the device. **CVE ID : CVE-2021-32514**	https://www.twcert.org.tw/tw/cp-132-4870-83620-1.html	A-QSA-STOR-200721/270
Exposure of Information Through Directory Listing	07-Jul-21	5	Directory listing vulnerability in share_link in QSAN Storage Manager allows attackers to list arbitrary directories and further access credential information. **CVE ID : CVE-2021-32515**	https://www.twcert.org.tw/tw/cp-132-4871-2a2d7-1.html	A-QSA-STOR-200721/271
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jul-21	5	Path traversal vulnerability in share_link in QSAN Storage Manager allows remote attackers to download arbitrary files. **CVE ID : CVE-2021-32516**	https://www.twcert.org.tw/tw/cp-132-4872-fcfa4-1.html	A-QSA-STOR-200721/272
Improper Access Control	07-Jul-21	5	Improper access control vulnerability in share_link in QSAN Storage Manager allows remote attackers to download arbitrary files using particular parameter in download function. **CVE ID : CVE-2021-32517**	https://www.twcert.org.tw/tw/cp-132-4873-6f88b-1.html	A-QSA-STOR-200721/273
UNIX Symbolic Link (Symlink) Following	07-Jul-21	5	A vulnerability in share_link in QSAN Storage Manager allows remote attackers to create a symbolic link then access arbitrary files. **CVE ID : CVE-2021-32518**	https://www.twcert.org.tw/tw/cp-132-4874-79edc-1.html	A-QSA-STOR-200721/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Password Hash With Insufficient Computational Effort	07-Jul-21	5	Use of password hash with insufficient computational effort vulnerability in QSAN Storage Manager, XEVO, SANOS allows remote attackers to recover the plain-text password by brute-forcing the MD5 hash. **CVE ID : CVE-2021-32519**	https://www.twcert.org.tw/tw/cp-132-4875-692f0-1.html	A-QSA-STOR-200721/275
Use of Hard-coded Credentials	07-Jul-21	7.5	Use of hard-coded cryptographic key vulnerability in QSAN Storage Manager allows attackers to obtain users' credentials and related permissions. **CVE ID : CVE-2021-32520**	https://www.twcert.org.tw/tw/cp-132-4876-8da07-1.html	A-QSA-STOR-200721/276
Use of Hard-coded Credentials	07-Jul-21	7.5	Use of MAC address as an authenticated password in QSAN Storage Manager, XEVO, SANOS allows local attackers to escalate privileges. **CVE ID : CVE-2021-32521**	https://www.twcert.org.tw/tw/cp-132-4877-7b696-1.html	A-QSA-STOR-200721/277
Improper Restriction of Excessive Authentication Attempts	07-Jul-21	5	Improper restriction of excessive authentication attempts vulnerability in QSAN Storage Manager, XEVO, SANOS allows remote attackers to discover users' credentials and obtain access via a brute force attack. **CVE ID : CVE-2021-32522**	https://www.twcert.org.tw/tw/cp-132-4878-0a279-1.html	A-QSA-STOR-200721/278
Improper Authorization	07-Jul-21	6.5	Improper authorization vulnerability in QSAN Storage Manager allows remote privileged users to bypass the access control	https://www.twcert.org.tw/tw/cp-132-4879-01616-	A-QSA-STOR-200721/279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and execute arbitrary commands. **CVE ID : CVE-2021-32523**	1.html	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	6.5	Command injection vulnerability in QSAN Storage Manager allows remote privileged users to execute arbitrary commands. **CVE ID : CVE-2021-32524**	https://www.twcert.org.tw/tw/cp-132-4880-e9ce7-1.html	A-QSA-STOR-200721/280
Use of Hard-coded Credentials	07-Jul-21	9	The same hard-coded password in QSAN Storage Manager's in the firmware allows remote attackers to access the control interface with the administrator's credential, entering the hard-coded password of the debug mode to execute the restricted system instructions. **CVE ID : CVE-2021-32525**	https://www.twcert.org.tw/tw/cp-132-4881-959d3-1.html	A-QSA-STOR-200721/281
Incorrect Permission Assignment for Critical Resource	07-Jul-21	4	Incorrect permission assignment for critical resource vulnerability in QSAN Storage Manager allows authenticated remote attackers to access arbitrary password files. **CVE ID : CVE-2021-32526**	https://www.twcert.org.tw/tw/cp-132-4882-c0310-1.html	A-QSA-STOR-200721/282
Improper Limitation of a Pathname to a Restricted Directory ('Path	07-Jul-21	5	Path traversal vulnerability in QSAN Storage Manager allows remote unauthenticated attackers to download arbitrary files thru injecting file path in download function.	https://www.twcert.org.tw/tw/cp-132-4883-aef9d-1.html	A-QSA-STOR-200721/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			**CVE ID : CVE-2021-32527**		
N/A	07-Jul-21	5	Observable behavioral discrepancy vulnerability in QSAN Storage Manager allows remote attackers to obtain the system information without permissions. **CVE ID : CVE-2021-32528**	https://www.twcert.org.tw/tw/cp-132-4884-fd4cb-1.html	A-QSA-STOR-200721/284
xevo					
Use of Password Hash With Insufficient Computational Effort	07-Jul-21	5	Use of password hash with insufficient computational effort vulnerability in QSAN Storage Manager, XEVO, SANOS allows remote attackers to recover the plain-text password by brute-forcing the MD5 hash. **CVE ID : CVE-2021-32519**	https://www.twcert.org.tw/tw/cp-132-4875-692f0-1.html	A-QSA-XEVO-200721/285
Use of Hard-coded Credentials	07-Jul-21	7.5	Use of MAC address as an authenticated password in QSAN Storage Manager, XEVO, SANOS allows local attackers to escalate privileges. **CVE ID : CVE-2021-32521**	https://www.twcert.org.tw/tw/cp-132-4877-7b696-1.html	A-QSA-XEVO-200721/286
Improper Restriction of Excessive Authentication Attempts	07-Jul-21	5	Improper restriction of excessive authentication attempts vulnerability in QSAN Storage Manager, XEVO, SANOS allows remote attackers to discover users' credentials and obtain access via a brute force attack. **CVE ID : CVE-2021-32522**	https://www.twcert.org.tw/tw/cp-132-4878-0a279-1.html	A-QSA-XEVO-200721/287
Improper Neutralizatio	07-Jul-21	7.5	Command injection vulnerability in QSAN XEVO,	https://www.twcert.org.	A-QSA-XEVO-200721/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			SANOS allows remote unauthenticated attackers to execute arbitrary commands. **CVE ID : CVE-2021-32529**	tw/tw/cp-132-4885-b03c8-1.html	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	7.5	OS command injection vulnerability in Array function in QSAN XEVO allows remote unauthenticated attackers to execute arbitrary commands via status parameter. **CVE ID : CVE-2021-32530**	https://www.twcert.org.tw/tw/cp-132-4886-d3b14-1.html	A-QSA-XEVO-200721/289
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	7.5	OS command injection vulnerability in Init function in QSAN XEVO allows remote attackers to execute arbitrary commands without permissions. **CVE ID : CVE-2021-32531**	https://www.twcert.org.tw/tw/cp-132-4887-ee5e3-1.html	A-QSA-XEVO-200721/290
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jul-21	5	Path traversal vulnerability in back-end analysis function in QSAN XEVO allows remote attackers to download arbitrary files without permissions. **CVE ID : CVE-2021-32532**	https://www.twcert.org.tw/tw/cp-132-4889-23410-1.html	A-QSA-XEVO-200721/291
Realtek					
hda_driver					
Improper Restriction of Operations within the	07-Jul-21	4.9	Realtek HAD contains a driver crashed vulnerability which allows local side attackers to send a special string to the kernel driver in	https://www.twcert.org.tw/tw/cp-132-4813-7b578-	A-REA-HDA_-200721/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			a user's mode. Due to unexpected commands, the kernel driver will cause the system crashed. A vulnerability in ___COMPONENT___ of Realtek HDA driver allows ___ATTACKER/ATTACK___ to cause ___IMPACT___. This issue affects: Realtek HDA driver 8155 version 9150 and prior versions. **CVE ID : CVE-2021-32537**	1.html	
record-like-deep-assign_project					
record-like-deep-assign					
Improperly Controlled Modification of Dynamically-Determined Object Attributes	02-Jul-21	7.5	All versions of package record-like-deep-assign are vulnerable to Prototype Pollution via the main functionality. **CVE ID : CVE-2021-23402**	https://snyk.io/vuln/SNYK-JS-RECORDLIKEDEEPASSIGN-1311024, https://github.com/kripod/record-like-deep-assign/blob/v1.0.1/src/mod.ts%23L17-L35	A-REC-RECO-200721/293
Redhat					
jboss_core_services					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity	09-Jul-21	4	A flaw was found in libxml2. Exponential entity expansion attack its possible bypassing all existing protection mechanisms and leading to denial of service. **CVE ID : CVE-2021-3541**	https://bugzilla.redhat.com/show_bug.cgi?id=1950515	A-RED-JBOS-200721/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Expansion')					
keycloak					
Allocation of Resources Without Limits or Throttling	09-Jul-21	5	A flaw was found in keycloak-model-infinispan in keycloak versions before 14.0.0 where authenticationSessions map in RootAuthenticationSessionEntity grows boundlessly which could lead to a DoS attack. **CVE ID : CVE-2021-3637**	https://bugzilla.redhat.com/show_bug.cgi?id=1979638	A-RED-KEYC-200721/295
single_sign-on					
Allocation of Resources Without Limits or Throttling	09-Jul-21	5	A flaw was found in keycloak-model-infinispan in keycloak versions before 14.0.0 where authenticationSessions map in RootAuthenticationSessionEntity grows boundlessly which could lead to a DoS attack. **CVE ID : CVE-2021-3637**	https://bugzilla.redhat.com/show_bug.cgi?id=1979638	A-RED-SING-200721/296
restsharp					
restsharp					
Incorrect Comparison	12-Jul-21	5	RestSharp < 106.11.8-alpha.0.13 uses a regular expression which is vulnerable to Regular Expression Denial of Service (ReDoS) when converting strings into DateTimes. If a server responds with a malicious string, the client using RestSharp will be stuck processing it for an	https://github.com/restsharp/RestSharp/issues/1556	A-RES-REST-200721/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exceedingly long time. Thus the remote server can trigger Denial of Service. **CVE ID : CVE-2021-27293**		
retty					
retty					
Missing Authorization	14-Jul-21	4.3	Improper authorization in handler for custom URL scheme vulnerability in Retty App for Android versions prior to 4.8.13 and Retty App for iOS versions prior to 4.11.14 allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App. **CVE ID : CVE-2021-20747**	N/A	A-RET-RETT-200721/298
salonbookingsystem					
salon_booking_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	4.3	The Salon booking system WordPress plugin before 6.3.1 does not properly sanitise and escape the First Name field when booking an appointment, allowing low privilege users such as subscriber to set JavaScript in them, leading to a Stored Cross-Site Scripting (XSS) vulnerability. The Payload will then be triggered when an admin visits the "Calendar" page and the malicious script is executed in the admin context. **CVE ID : CVE-2021-24429**	https://wpscan.com/vulnerability/e922b788-7da5-43b4-9b05-839c8610252a	A-SAL-SALO-200721/299
Samsung					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ar_emoji_editor					
Improper Input Validation	08-Jul-21	4.6	Improper input validation vulnerability in AR Emoji Editor prior to version 4.4.03.5 in Android Q(10.0) and above allows untrusted applications to access arbitrary files with an escalated privilege. **CVE ID : CVE-2021-25441**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	A-SAM-AR_E-200721/300
cameralyzer					
Incorrect Authorization	08-Jul-21	2.1	Improper access control vulnerability in Cameralyzer prior to versions 3.2.1041 in 3.2.x, 3.3.1040 in 3.3.x, and 3.4.4210 in 3.4.x allows untrusted applications to access some functions of Cameralyzer. **CVE ID : CVE-2021-25431**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	A-SAM-CAME-200721/301
factorycamerafb					
Incorrect Authorization	08-Jul-21	4.6	Improper access control vulnerability in FactoryCameraFB prior to version 3.4.74 allows untrusted applications to access arbitrary files with an escalated privilege. **CVE ID : CVE-2021-25440**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	A-SAM-FACT-200721/302
knox_cloud_services					
Improper Authentication	08-Jul-21	5	Improper MDM policy management vulnerability in KME module prior to KCS version 1.39 allows MDM users to bypass Knox Manage authentication. **CVE ID : CVE-2021-25442**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	A-SAM-KNOX-200721/303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
members					
Incorrect Authorization	08-Jul-21	4.6	Improper access control vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to cause local file inclusion in webview. **CVE ID : CVE-2021-25438**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	A-SAM-MEMB-200721/304
Incorrect Authorization	08-Jul-21	2.1	Improper access control vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to cause arbitrary webpage loading in webview. **CVE ID : CVE-2021-25439**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	A-SAM-MEMB-200721/305
samsung_members					
Exposure of Resource to Wrong Sphere	08-Jul-21	2.1	Information exposure vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to access chat data. **CVE ID : CVE-2021-25432**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	A-SAM-SAMS-200721/306
Siemens					
jt2go					
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2),	https://cert-portal.siemens.com/prod	A-SIE-JT2G-200721/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12956) **CVE ID : CVE-2021-34291**	uctcert/pdf/ssa-483182.pdf	
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12959) **CVE ID : CVE-2021-34292**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/308
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13020) **CVE ID : CVE-2021-34293**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13023 **CVE ID : CVE-2021-34294**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/310
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13024) **CVE ID : CVE-2021-34295**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13057) **CVE ID : CVE-2021-34296**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/312
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the current process. (ZDI-CAN-13059) **CVE ID : CVE-2021-34297**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing BMP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13060) **CVE ID : CVE-2021-34298**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/314
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13192) **CVE ID : CVE-2021-34299**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/315
Improper	13-Jul-21	6.8	A vulnerability has been	https://cert-	A-SIE-JT2G-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13194) **CVE ID : CVE-2021-34300**	portal.siemens.com/productcert/pdf/ssa-483182.pdf	200721/316
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing BMP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13196) **CVE ID : CVE-2021-34301**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/317
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13197) **CVE ID : CVE-2021-34302**		
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13198) **CVE ID : CVE-2021-34303**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/319
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13199) **CVE ID : CVE-2021-34304**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13340) **CVE ID : CVE-2021-34305**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/321
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the current process. (ZDI-CAN-13342) **CVE ID : CVE-2021-34306**		
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13343) **CVE ID : CVE-2021-34307**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/323
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13344) **CVE ID : CVE-2021-34308**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13350) **CVE ID : CVE-2021-34309**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/325
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13351) **CVE ID : CVE-2021-34310**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/326
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization	https://cert-portal.siemens.com/productcert/pdf/	A-SIE-JT2G-200721/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V13.2). The Mono_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13352) **CVE ID : CVE-2021-34311**	ssa-483182.pdf	
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13353) **CVE ID : CVE-2021-34312**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/328
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13354) **CVE ID : CVE-2021-34313**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13355) **CVE ID : CVE-2021-34314**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/330
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds read past the end of an allocated	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13356) **CVE ID : CVE-2021-34315**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The DL180CoolType.dll library in affected applications lacks proper validation of user-supplied data when parsing PDF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13380) **CVE ID : CVE-2021-34316**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/332
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCX files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CAN-13402) **CVE ID : CVE-2021-34317**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13403) **CVE ID : CVE-2021-34318**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/334
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13404) **CVE ID : CVE-2021-34319**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/335
Improper	13-Jul-21	4.3	A vulnerability has been	https://cert-	A-SIE-JT2G-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13406) **CVE ID : CVE-2021-34320**	portal.siemens.com/productcert/pdf/ssa-483182.pdf	200721/336
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The VisDraw.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13414) **CVE ID : CVE-2021-34321**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/337
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The	https://cert-portal.siemens.com/productcert/pdf/ssa-	A-SIE-JT2G-200721/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			JPEG2K_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13416) **CVE ID : CVE-2021-34322**	483182.pdf	
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13419) **CVE ID : CVE-2021-34323**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/339
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			object when parsing JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13420) **CVE ID : CVE-2021-34324**		
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13421) **CVE ID : CVE-2021-34325**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/341
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-173615.pdf	A-SIE-JT2G-200721/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13422) **CVE ID : CVE-2021-34326**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing ASM files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13423) **CVE ID : CVE-2021-34327**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-173615.pdf	A-SIE-JT2G-200721/343
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-173615.pdf	A-SIE-JT2G-200721/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13424) **CVE ID : CVE-2021-34328**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13427) **CVE ID : CVE-2021-34329**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-173615.pdf	A-SIE-JT2G-200721/345
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13430) **CVE ID : CVE-2021-34330**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13442) **CVE ID : CVE-2021-34331**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/347
Loop with Unreachable Exit Condition ('Infinite Loop')	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in an infinite loop condition that leads to denial of service condition. An attacker could leverage this vulnerability to consume excessive resources. (CNVD-C-2021-79300) **CVE ID : CVE-2021-34332**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-JT2G-200721/348
Double Free	13-Jul-21	4.3	A vulnerability has been	https://cert-	A-SIE-JT2G-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in double free of an allocated buffer that leads to a crash. An attacker could leverage this vulnerability to cause denial of service condition. (CNVD-C-2021-79295) **CVE ID : CVE-2021-34333**	portal.siemens.com/productcert/pdf/ssa-483182.pdf	200721/349
solid_edge					
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13422) **CVE ID : CVE-2021-34326**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-173615.pdf	A-SIE-SOLI-200721/350
Improper	13-Jul-21	6.8	A vulnerability has been	https://cert-	A-SIE-SOLI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing ASM files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13423) **CVE ID : CVE-2021-34327**	portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-173615.pdf	200721/351
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13424) **CVE ID : CVE-2021-34328**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-173615.pdf	A-SIE-SOLI-200721/352
Improper	13-Jul-21	6.8	A vulnerability has been	https://cert-	A-SIE-SOLI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13427) **CVE ID : CVE-2021-34329**	portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-173615.pdf	200721/353
teamcenter_visualization					
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12956) **CVE ID : CVE-2021-34291**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/354
Improper	13-Jul-21	6.8	A vulnerability has been	https://cert-	A-SIE-TEAM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12959) **CVE ID : CVE-2021-34292**	portal.siemens.com/productcert/pdf/ssa-483182.pdf	200721/355
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13020) **CVE ID : CVE-2021-34293**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/356
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The	https://cert-portal.siemens.com/productcert/pdf/ssa-	A-SIE-TEAM-200721/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13023 **CVE ID : CVE-2021-34294**	483182.pdf	
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13024) **CVE ID : CVE-2021-34295**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/358
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13057) **CVE ID : CVE-2021-34296**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13059) **CVE ID : CVE-2021-34297**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/360
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing BMP files. An attacker could leverage this	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to execute code in the context of the current process. (ZDI-CAN-13060) **CVE ID : CVE-2021-34298**		
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13192) **CVE ID : CVE-2021-34299**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/362
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13194)	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34300		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing BMP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13196) **CVE ID : CVE-2021-34301**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/364
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13197) **CVE ID : CVE-2021-34302**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/365
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2),	https://cert-portal.siemens.com/prod	A-SIE-TEAM-200721/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13198) **CVE ID : CVE-2021-34303**	uctcert/pdf/ssa-483182.pdf	
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13199) **CVE ID : CVE-2021-34304**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/367
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13340) **CVE ID : CVE-2021-34305**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13342) **CVE ID : CVE-2021-34306**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/369
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13343) **CVE ID : CVE-2021-34307**		
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13344) **CVE ID : CVE-2021-34308**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/371
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CAN-13350) **CVE ID : CVE-2021-34309**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13351) **CVE ID : CVE-2021-34310**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/373
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Mono_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13352) **CVE ID : CVE-2021-34311**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/374
Improper	13-Jul-21	6.8	A vulnerability has been	https://cert-	A-SIE-TEAM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13353) **CVE ID : CVE-2021-34312**	portal.siemens.com/productcert/pdf/ssa-483182.pdf	200721/375
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13354) **CVE ID : CVE-2021-34313**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/376
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The	https://cert-portal.siemens.com/productcert/pdf/ssa-	A-SIE-TEAM-200721/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13355) **CVE ID : CVE-2021-34314**	483182.pdf	
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13356) **CVE ID : CVE-2021-34315**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/378
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The DL180CoolType.dll library in affected applications lacks proper validation of user-supplied data when parsing	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PDF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13380) **CVE ID : CVE-2021-34316**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCX files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13402) **CVE ID : CVE-2021-34317**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/380
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13403) **CVE ID : CVE-2021-34318**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13404) **CVE ID : CVE-2021-34319**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/382
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13406)	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34320		
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The VisDraw.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13414) **CVE ID : CVE-2021-34321**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/384
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The JPEG2K_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13416) **CVE ID : CVE-2021-34322**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/385
Improper Input	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All	https://cert-portal.sieme	A-SIE-TEAM-200721/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13419) **CVE ID : CVE-2021-34323**	ns.com/productcert/pdf/ssa-483182.pdf	
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13420) **CVE ID : CVE-2021-34324**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/387
Improper Input Validation	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data when parsing JT files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13421) **CVE ID : CVE-2021-34325**		
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13422) **CVE ID : CVE-2021-34326**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-173615.pdf	A-SIE-TEAM-200721/389
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/	A-SIE-TEAM-200721/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied data when parsing ASM files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13423) **CVE ID : CVE-2021-34327**	ssa-173615.pdf	
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13424) **CVE ID : CVE-2021-34328**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/ssa-173615.pdf	A-SIE-TEAM-200721/391
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf, https://cert-portal.siemens.com/productcert/pdf/	A-SIE-TEAM-200721/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13427) **CVE ID : CVE-2021-34329**	ssa-173615.pdf	
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13430) **CVE ID : CVE-2021-34330**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/393
Improper Input Validation	13-Jul-21	6.8	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to execute code in the context of the current process. (ZDI-CAN-13442) **CVE ID : CVE-2021-34331**		
Loop with Unreachable Exit Condition ('Infinite Loop')	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in an infinite loop condition that leads to denial of service condition. An attacker could leverage this vulnerability to consume excessive resources. (CNVD-C-2021-79300) **CVE ID : CVE-2021-34332**	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/395
Double Free	13-Jul-21	4.3	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in double free of an allocated buffer that leads to a crash. An attacker could leverage this vulnerability to cause denial of service condition. (CNVD-C-2021-79295)	https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf	A-SIE-TEAM-200721/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34333		
sitasoftware					
azurcms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jul-21	6.5	A SQL injection vulnerability in azurWebEngine in Sita AzurCMS through 1.2.3.12 allows an authenticated attacker to execute arbitrary SQL commands via the id parameter to mesdocs.ajax.php in azurWebEngine/eShop. By default, the query is executed as DBA. **CVE ID : CVE-2021-27950**	https://www.sitasoftware.lu/azur/software/web.php, https://www.sitasoftware.lu/	A-SIT-AZUR-200721/397
Smartertools					
smartermail					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-21	4.3	SmarterTools SmarterMail before Build 7776 allows XSS. **CVE ID : CVE-2021-32233**	https://www.smartertools.com/smartermail/release-notes/current	A-SMA-SMAR-200721/398
smashing_project					
smashing					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jul-21	4.3	Smashing 1.3.4 is vulnerable to Cross Site Scripting (XSS). A URL for a widget can be crafted and used to execute JavaScript on the victim's computer. The JavaScript code can then steal data available in the session/cookies depending on the user environment (e.g. if re-using internal	https://github.com/Smashing/smashing/pull/186#issuecomment-871727614, https://github.com/Smashing/smashi	A-SMA-SMAS-200721/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			URL's for deploying, or cookies that are very permissive) private information may be retrieved by the attacker. **CVE ID : CVE-2021-35440**	ng/pull/186	
smooth_scroll_page_up\\/down_buttons_project					
Solarwinds					
dameware_mini_remote_control					
Incorrect Default Permissions	13-Jul-21	9.4	In SolarWinds DameWare Mini Remote Control Server 12.0.1.200, insecure file permissions allow file deletion as SYSTEM. **CVE ID : CVE-2021-31217**	https://support.solarwinds.com/SuccessCenter/s/, https://documentation.solarwinds.com/en/success_center/dameware/content/release_notes/dameware_12-2_release_notes.htm	A-SOL-DAME-200721/400
splinterware					
system_scheduler					
Improper Privilege Management	06-Jul-21	7.2	Splinterware System Scheduler Professional version 5.30 is subject to insecure folders permissions issue impacting where the service 'WindowsScheduler' calls its executable. This allow a non-privileged user to execute arbitrary code with elevated privileges (system level privileges as	http://splinterware.com	A-SPL-SYST-200721/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"nt authority\system") since the service runs as Local System. **CVE ID : CVE-2021-31771**		
stellar					
js-stellar-sdk					
Improper Authentication	02-Jul-21	4	js-stellar-sdk is a Javascript library for communicating with a Stellar Horizon server. The `Utils.readChallengeTx` function used in SEP-10 Stellar Web Authentication states in its function documentation that it reads and validates the challenge transaction including verifying that the `serverAccountID` has signed the transaction. In js-stellar-sdk before version 8.2.3, the function does not verify that the server has signed the transaction. Applications that also used `Utils.verifyChallengeTxThreshold` or `Utils.verifyChallengeTxSigners` to verify the signatures including the server signature on the challenge transaction are unaffected as those functions verify the server signed the transaction. Applications calling `Utils.readChallengeTx` should update to version 8.2.3, the first version with a patch for this vulnerability,	https://github.com/stellar/js-stellar-sdk/security/advisories/GHSA-6cgh-hjpw-q3gq	A-STE-JS-S-200721/402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to ensure that the challenge transaction is completely valid and signed by the server creating the challenge transaction. **CVE ID : CVE-2021-32738**		
stockware					
motor					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jul-21	7.5	Lack of authentication or validation in motor_load_more, motor_gallery_load_more, motor_quick_view and motor_project_quick_view AJAX handlers of the Motor WordPress theme before 3.1.0 allows an unauthenticated attacker access to arbitrary files in the server file system, and to execute arbitrary php scripts found on the server file system. We found no vulnerability for uploading files with this theme, so any scripts to be executed must already be on the server file system. **CVE ID : CVE-2021-24375**	https://wpscan.com/vulnerability/d9518429-79d3-4b13-88ff-3722d05efa9f	A-STO-MOTO-200721/403
stormshield					
endpoint_security					
N/A	13-Jul-21	2.3	SES Evolution before 2.1.0 allows modifying security policies by leveraging access of a user having read-only access to security policies. **CVE ID : CVE-2021-31220**	https://advisories.stormshield.eu, https://advisories.stormshield.eu/2021-022/	A-STO-ENDP-200721/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Jul-21	2.9	SES Evolution before 2.1.0 allows deleting some parts of a security policy by leveraging access to a computer having the administration console installed. **CVE ID : CVE-2021-31221**	https://advisories.stormshield.eu, https://advisories.stormshield.eu/2021-023/	A-STO-ENDP-200721/405
N/A	13-Jul-21	2.9	SES Evolution before 2.1.0 allows updating some parts of a security policy by leveraging access to a computer having the administration console installed. **CVE ID : CVE-2021-31222**	https://advisories.stormshield.eu, https://advisories.stormshield.eu/2021-024/	A-STO-ENDP-200721/406
N/A	13-Jul-21	2.9	SES Evolution before 2.1.0 allows reading some parts of a security policy by leveraging access to a computer having the administration console installed. **CVE ID : CVE-2021-31223**	https://advisories.stormshield.eu/2021-025/, https://advisories.stormshield.eu	A-STO-ENDP-200721/407
N/A	13-Jul-21	2.9	SES Evolution before 2.1.0 allows duplicating an existing security policy by leveraging access of a user having read-only access to security policies. **CVE ID : CVE-2021-31224**	https://advisories.stormshield.eu/2021-026/, https://advisories.stormshield.eu	A-STO-ENDP-200721/408
N/A	13-Jul-21	4.3	SES Evolution before 2.1.0 allows deleting some resources not currently in use by any security policy by leveraging access to a computer having the administration console	https://advisories.stormshield.eu/2021-027/, https://advisories.stormshield.eu	A-STO-ENDP-200721/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installed. **CVE ID : CVE-2021-31225**		
Uncontrolled Search Path Element	13-Jul-21	4.6	Stormshield Endpoint Security Evolution 2.0.0 through 2.0.2 does not accomplish the intended defense against local administrators who can replace the Visual C++ runtime DLLs (in %WINDIR%\system32) with malicious ones. **CVE ID : CVE-2021-35957**	https://advisories.stormshield.eu, https://advisories.stormshield.eu/2021-045/	A-STO-ENDP-200721/410
stormshield_network_security					
Improper Restriction of Excessive Authentication Attempts	01-Jul-21	5	An issue was discovered in Stormshield SNS through 4.2.1. A brute-force attack can occur. **CVE ID : CVE-2021-28127**	https://advisories.stormshield.eu/2021-006, https://advisories.stormshield.eu	A-STO-STOR-200721/411
sulu					
sulu					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-21	3.5	Sulu is an open-source PHP content management system based on the Symfony framework. In versions of Sulu prior to 1.6.41, it is possible for a logged in admin user to add a script injection (cross-site-scripting) in the collection title. The problem is patched in version 1.6.41. As a workaround, one may manually patch the affected JavaScript files in lieu of updating.	https://github.com/sulu/sulu/security/advisories/GHSA-gm2x-6475-g9r8	A-SUL-SULU-200721/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-32737		
tcl					
tcl					
Use of Externally-Controlled Format String	05-Jul-21	6.8	** DISPUTED ** In Tcl 8.6.11, a format string vulnerability in nmakehlp.c might allow code execution via a crated file. NOTE: multiple third parties dispute the significance of this finding. **CVE ID : CVE-2021-35331**	https://core.tcl-lang.org/tcl/info/28ef6c0c741408a2, https://core.tcl-lang.org/tcl/info/bad6cc213dfe8280, https://github.com/tcltk/tcl/commit/4705dbdde2f32ff90420765cd93e7ac71d81a222	A-TCL-TCL-200721/413
teachers_record_management_system_project					
teachers_record_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Jul-21	6.5	Multiple SQL Injection vulnerabilities in Teachers Record Management System 1.0 allow remote authenticated users to execute arbitrary SQL commands via the 'editid' GET parameter in edit-subjects-detail.php, edit-teacher-detail.php, or the 'searchdata' POST parameter in search.php. **CVE ID : CVE-2021-28423**	N/A	A-TEA-TEAC-200721/414
Improper Neutralization of Input	01-Jul-21	3.5	A stored cross-site scripting (XSS) vulnerability in Teachers Record	N/A	A-TEA-TEAC-200721/415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Management System 1.0 allows remote authenticated users to inject arbitrary web script or HTML via the 'email' POST parameter in adminprofile.php. **CVE ID : CVE-2021-28424**		
teradici					
pcoip_management_console					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-21	4.3	In Teradici PCoIP Management Console-Enterprise 20.07.0, an unauthenticated user can inject arbitrary text into user browser via the Web application. **CVE ID : CVE-2021-35451**	http://teradici.com	A-TER-PCOI-200721/416
tesseract_ocr_project					
tesseract_ocr					
Use After Free	01-Jul-21	6.8	Tesseract OCR 5.0.0-alpha-20201231 has a one_ell_conflict use-after-free during a strpbrk call. **CVE ID : CVE-2021-36081**	https://github.com/tesseract-ocr/tesseract/commit/e6f15621c2ab2ecbfabf656942d8ef66f03b2d55, https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=29698	A-TES-TESS-200721/417
tielabs					
jannah					
Improper	06-Jul-21	4.3	The Jannah WordPress	https://wpsc	A-TIE-JANN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			theme before 5.4.5 did not properly sanitize the 'query' POST parameter in its tie_ajax_search AJAX action, leading to a Reflected Cross-site Scripting (XSS) vulnerability. **CVE ID : CVE-2021-24407**	an.com/vulnerability/fba9f010-1202-4eea-a6f5-7886c084153	200721/418
Tipsandtricks-hq					
software_license_manager					
Cross-Site Request Forgery (CSRF)	14-Jul-21	6.8	Cross-site request forgery (CSRF) vulnerability in Software License Manager versions prior to 4.4.6 allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2021-20782**	https://www.tipsandtricks-hq.com/software-license-manager-plugin-for-wordpress	A-TIP-SOFT-200721/419
totaljs					
total.js					
Improper Control of Generation of Code ('Code Injection')	12-Jul-21	7.5	The package total.js before 3.4.9 are vulnerable to Arbitrary Code Execution via the U.set() and U.get() functions. **CVE ID : CVE-2021-23389**	https://github.com/totaljs/framework/commit/887b0fa9e162ef7a2dd9cec20a5ca122726373b3, https://snyk.io/vuln/SNYK-JS-TOTALJS-1088607	A-TOT-TOTA-200721/420
total4					
Improper Control of Generation	12-Jul-21	7.5	The package total4 before 0.0.43 are vulnerable to Arbitrary Code Execution via	https://snyk.io/vuln/SNYK-JS-	A-TOT-TOTA-200721/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			the U.set() and U.get() functions. **CVE ID : CVE-2021-23390**	TOTAL4-1130527, https://github.com/totaljs/framework4/commit/8a72d8c20f38bbcac031a76a51238aa528f68821	
treasuredata					
fluent_bit					
Double Free	01-Jul-21	7.5	Fluent Bit (aka fluent-bit) 1.7.0 through 1.7,4 has a double free in flb_free (called from flb_parser_json_do and flb_parser_do). **CVE ID : CVE-2021-36088**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=33750, https://github.com/fluent/fluent-bit/commit/22346a74c07ceb90296be872be2d53eb92252a54, https://github.com/fluent/fluent-bit/pull/3453	A-TRE-FLUE-200721/422
ts-nodash_project					
ts-nodash					
Improperly Controlled Modification of Dynamically-Determined	02-Jul-21	7.5	All versions of package ts-nodash are vulnerable to Prototype Pollution via the Merge() function due to lack of validation input.	N/A	A-TS--TS-N-200721/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Object Attributes			**CVE ID : CVE-2021-23403**		
voidtools					
everything					
N/A	14-Jul-21	5.8	HTTP header injection vulnerability in Everything all versions except the Lite version may allow a remote attacker to inject an arbitrary script or alter the website that uses the product via unspecified vectors. **CVE ID : CVE-2021-20784**	https://www.voidtools.com/, https://www.voidtools.com/downloads/	A-VOI-EVER-200721/424
Web-dorado					
backup-wd					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	3.5	The Backup by 10Web â€“ Backup and Restore Plugin WordPress plugin through 1.0.20 does not sanitise or escape the tab parameter before outputting it back in the page, leading to a reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24426**	https://wpscan.com/vulnerability/48464b3f-fe57-40fe-8868-398a36099fb9	A-WEB-BACK-200721/425
webfactoryltd					
wp_reset					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	3.5	The WP Reset â€“ Most Advanced WordPress Reset Tool WordPress plugin before 1.90 did not sanitise or escape its extra_data parameter when creating a snapshot via the admin dashboard, leading to an authenticated Stored Cross-	https://wpscan.com/vulnerability/90cf8f9d-4d37-405d-b161-239bdb281828	A-WEB-WP_R-200721/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Site Scripting issue **CVE ID : CVE-2021-24424**		
Webkitgtk					
webkitgtk					
Use After Free	07-Jul-21	6.8	A use-after-free vulnerability exists in the way certain events are processed for ImageLoader objects of Webkit WebKitGTK 2.30.4. A specially crafted web page can lead to a potential information leak and further memory corruption. In order to trigger the vulnerability, a victim must be tricked into visiting a malicious webpage. **CVE ID : CVE-2021-21775**	N/A	A-WEB-WEBK-200721/427
Use After Free	08-Jul-21	6.8	A use-after-free vulnerability exists in the way Webkit's GraphicsContext handles certain events in WebKitGTK 2.30.4. A specially crafted web page can lead to a potential information leak and further memory corruption. A victim must be tricked into visiting a malicious web page to trigger this vulnerability. **CVE ID : CVE-2021-21779**	N/A	A-WEB-WEBK-200721/428
Use After Free	08-Jul-21	6.8	An exploitable use-after-free vulnerability exists in WebKitGTK browser version 2.30.3 x64. A specially crafted HTML web page can cause a use-after-free condition, resulting in	N/A	A-WEB-WEBK-200721/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote code execution. The victim needs to visit a malicious web site to trigger the vulnerability. **CVE ID : CVE-2021-21806**		
wp-currency					
wordpress_currency_switcher					
Cross-Site Request Forgery (CSRF)	07-Jul-21	6.8	Cross-site request forgery (CSRF) vulnerability in WPCS - WordPress Currency Switcher 1.1.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2021-20780**	N/A	A-WP--WORD-200721/430
wp-upload-restriction_project					
wp-upload-restriction					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jul-21	3.5	A vulnerability in the saveCustomType function of the WP Upload Restriction WordPress plugin allows low-level authenticated users to inject arbitrary web scripts. This issue affects versions 2.2.3 and prior. **CVE ID : CVE-2021-34625**	N/A	A-WP--WP-U-200721/431
Incorrect Authorization	07-Jul-21	4	A vulnerability in the deleteCustomType function of the WP Upload Restriction WordPress plugin allows low-level authenticated users to delete custom extensions added by administrators. This issue affects versions 2.2.3 and prior.	N/A	A-WP--WP-U-200721/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34626		
Incorrect Authorization	07-Jul-21	3.5	A vulnerability in the getSelectedMimeTypesByRole function of the WP Upload Restriction WordPress plugin allows low-level authenticated users to view custom extensions added by administrators. This issue affects versions 2.2.3 and prior. **CVE ID : CVE-2021-34627**	N/A	A-WP--WP-U-200721/433
wpdevart					
poll\\,_survey\\,_questionnaire_and_voting_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Jul-21	7.5	The Poll, Survey, Questionnaire and Voting system WordPress plugin before 1.5.3 did not sanitise, escape or validate the date_answers[] POST parameter before using it in a SQL statement when sending a Poll result, allowing unauthenticated users to perform SQL Injection attacks **CVE ID : CVE-2021-24442**	https://wpscan.com/vulnerability/7376666e-9b2a-4239-b11f-8544435b444a	A-WPD-POLL-200721/434
wp_youtube_lyte_project					
wp_youtube_lyte					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	3.5	The WP YouTube Lyte WordPress plugin before 1.7.16 did not sanitise or escape its lyte_yt_api_key and lyte_notification settings before outputting them back in the page, allowing high privilege users to set XSS payload on them and leading	https://wpscan.com/vulnerability/0eeff1ee-d11e-4d52-a032-5f5bd8a6a2d7	A-WP_-WP_Y-200721/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to stored Cross-Site Scripting issues. **CVE ID : CVE-2021-24419**		
xen-orchestra					
xo-server					
Incorrect Authorization	12-Jul-21	4	Xen Orchestra (with xo-web through 5.80.0 and xo-server through 5.84.0) mishandles authorization, as demonstrated by modified WebSocket resourceSet.getAll data is which the attacker changes the permission field from none to admin. The attacker gains access to data sets such as VMs, Backups, Audit, Users, and Groups. **CVE ID : CVE-2021-36383**	N/A	A-XEN-XO-S-200721/436
xo-web					
Incorrect Authorization	12-Jul-21	4	Xen Orchestra (with xo-web through 5.80.0 and xo-server through 5.84.0) mishandles authorization, as demonstrated by modified WebSocket resourceSet.getAll data is which the attacker changes the permission field from none to admin. The attacker gains access to data sets such as VMs, Backups, Audit, Users, and Groups. **CVE ID : CVE-2021-36383**	N/A	A-XEN-XO-W-200721/437
Xmlsoft					
libxml2					
Improper	09-Jul-21	4	A flaw was found in libxml2.	https://bugz	A-XML-LIBX-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')			Exponential entity expansion attack its possible bypassing all existing protection mechanisms and leading to denial of service. **CVE ID : CVE-2021-3541**	illa.redhat.com/show_bug.cgi?id=1950515	200721/438
Xwiki					
Xwiki					
Improper Authentication	01-Jul-21	5.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A vulnerability exists in versions prior to 12.6.88, 12.10.4, and 13.0. The script service method used to reset the authentication failures record can be executed by any user with Script rights and does not require Programming rights. An attacher with script rights who is able to reset the authentication failure record might perform a brute force attack, since they would be able to virtually deactivate the mechanism introduced to mitigate those attacks. The problem has been patched in version 12.6.8, 12.10.4 and 13.0. There are no workarounds aside from upgrading. **CVE ID : CVE-2021-32729**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-m738-3rc4-5xv3, https://jira.xwiki.org/browse/XWIKI-18276	A-XWI-XWIK-200721/439
Cross-Site Request Forgery	01-Jul-21	4.3	XWiki Platform is a generic wiki platform offering runtime services for	https://github.com/xwiki/xwiki-	A-XWI-XWIK-200721/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			applications built on top of it. A cross-site request forgery vulnerability exists in versions prior to 12.10.5, and in versions 13.0 through 13.1. It's possible for forge an URL that, when accessed by an admin, will reset the password of any user in XWiki. The problem has been patched in XWiki 12.10.5 and 13.2RC1. As a workaround, it is possible to apply the patch manually by modifying the `register_macros.vm` template. **CVE ID : CVE-2021-32730**	platform/security/advisories/GHSA-v9j2-q4q5-cxh4, https://github.com/xwiki/xwiki-platform/commit/0a36dbcc5421d450366580217a47cc44d32f7257, https://jira.xwiki.org/browse/XWIKI-18315	
Exposure of Resource to Wrong Sphere	01-Jul-21	5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Between (and including) versions 13.1RC1 and 13.1, the reset password form reveals the email address of users just by giving their username. The problem has been patched on XWiki 13.2RC1. As a workaround, it is possible to manually modify the `resetpasswordinline.vm` to perform the changes made to mitigate the vulnerability. **CVE ID : CVE-2021-32731**	https://github.com/xwiki/xwiki-platform/commit/0cf716250b3645a5974c80d8336dcdf885749dff#diff-14a3132e3986b1f5606dd13d9d8a8bb8634bec9932123c5e49e9604cfd850fc2, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-	A-XWI-XWIK-200721/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				h4m4-pgp4-whgm	
yop-poll					
yop_poll					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Jul-21	4.3	In the YOP Poll WordPress plugin before 6.2.8, when a pool is created with the options "Allow other answers", "Display other answers in the result list" and "Show results", it can lead to Stored Cross-Site Scripting issues as the 'Other' answer is not sanitised before being output in the page. The execution of the XSS payload depends on the 'Show results' option selected, which could be before or after sending the vote for example. **CVE ID : CVE-2021-24454**	https://wpscan.com/vulnerability/48ade7a5-5abb-4267-b9b6-13e31e1b3e91	A-YOP-YOP_-200721/442
Zimbra					
collaboration					
URL Redirection to Untrusted Site ('Open Redirect')	02-Jul-21	5.8	An open redirect vulnerability exists in the /preauth Servlet in Zimbra Collaboration Suite through 9.0. To exploit the vulnerability, an attacker would need to have obtained a valid zimbra auth token or a valid preauth token. Once the token is obtained, an attacker could redirect a user to any URL via isredirect=1&redirectURL= in conjunction with the	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P23, https://wiki.zimbra.com/wiki/Security_Center,	A-ZIM-COLL-200721/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			token data (e.g., a valid authtoken= value). **CVE ID : CVE-2021-34807**	https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P16	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-21	4.3	An issue was discovered in Zimbra Collaboration Suite 8.8 before 8.8.15 Patch 23 and 9.0 before 9.0.0 Patch 16. An XSS vulnerability exists in the login component of Zimbra Web Client, in which an attacker can execute arbitrary JavaScript by adding executable JavaScript to the loginErrorCode parameter of the login url. **CVE ID : CVE-2021-35207**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P23, https://wiki.zimbra.com/wiki/Security_Center, https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P16	A-ZIM-COLL-200721/444
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jul-21	3.5	An issue was discovered in ZmMailMsgView.js in the Calendar Invite component in Zimbra Collaboration Suite 8.8.x before 8.8.15 Patch 23. An attacker could place HTML containing executable JavaScript inside element attributes. This markup becomes unescaped, causing arbitrary markup to be injected into the document. **CVE ID : CVE-2021-35208**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P23, https://wiki.zimbra.com/wiki/Security_Center, https://wiki.zimbra.com/	A-ZIM-COLL-200721/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				wiki/Zimbra_Releases/9.0.0/P16	
URL Redirection to Untrusted Site ('Open Redirect')	02-Jul-21	5.8	An issue was discovered in ProxyServlet.java in the /proxy servlet in Zimbra Collaboration Suite 8.8 before 8.8.15 Patch 23 and 9.x before 9.0.0 Patch 16. The value of the X-Host header overwrites the value of the Host header in proxied requests. The value of X-Host header is not checked against the whitelist of hosts Zimbra is allowed to proxy to (the zimbraProxyAllowedDomains setting). **CVE ID : CVE-2021-35209**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P23, https://wiki.zimbra.com/wiki/Security_Center, https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P16	A-ZIM-COLL-200721/446
Zohocorp					
manageengine_adselfservice_plus					
N/A	02-Jul-21	4.3	Zoho ManageEngine ADSelfService Plus before 6104, in rare situations, allows attackers to obtain sensitive information about the password-sync database application. **CVE ID : CVE-2021-31874**	https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6104-released-with-an-important-security-fixes	A-ZOH-MANA-200721/447
manageengine_applications_manager					
Improper Neutralization of Input	01-Jul-21	3.5	Zoho ManageEngine Applications Manager before 15130 is vulnerable to	https://www.manageengine.com/pr	A-ZOH-MANA-200721/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Stored XSS while importing malicious user details (e.g., a crafted user name) from AD. **CVE ID : CVE-2021-31813**	oducts/applications_manager/security-updates/security-updates-cve-2021-31813.html	
Zope					
grok					
Out-of-bounds Write	01-Jul-21	6.8	Grok 7.6.6 through 9.2.0 has a heap-based buffer overflow in grk::FileFormatDecompress::apply_palette_clr (called from grk::FileFormatDecompress::applyColour). **CVE ID : CVE-2021-36089**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=33544	A-ZOP-GROK-200721/449
Hardware					
a-stage-inc					
at-40cm01sr					
Improper Authentication	07-Jul-21	7.5	Improper authentication vulnerability in SCT-40CM01SR and AT-40CM01SR allows an attacker to bypass access restriction and execute an arbitrary command via telnet. **CVE ID : CVE-2021-20776**	N/A	H-A-S-AT-4-190721/450
sct-40cm01sr					
Improper Authentication	07-Jul-21	7.5	Improper authentication vulnerability in SCT-40CM01SR and AT-40CM01SR allows an	N/A	H-A-S-SCT--190721/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass access restriction and execute an arbitrary command via telnet. **CVE ID : CVE-2021-20776**		
Cisco					
video_surveillance_7070					
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	H-CIS-VIDE-190721/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent). **CVE ID : CVE-2021-1595**		
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1596**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	H-CIS-VIDE-190721/453
Missing Release of Memory	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP)	https://tools.cisco.com/security/center	H-CIS-VIDE-190721/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1597**	/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-	H-CIS-VIDE-190721/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1598**	wGqundTq	
video_surveillance_7530pd					
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	H-CIS-VIDE-190721/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1595**		
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	H-CIS-VIDE-190721/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1596**		
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	H-CIS-VIDE-190721/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1597**		
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	H-CIS-VIDE-190721/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1598**		
elecom					
wrc-1167fs-b					
N/A	07-Jul-21	3.3	WRC-1167FS-W, WRC-1167FS-B, and WRC-1167FSA all versions allow an unauthenticated network-adjacent attacker to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2021-20738**	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRC--190721/460
wrc-1167fs-w					
N/A	07-Jul-21	3.3	WRC-1167FS-W, WRC-1167FS-B, and WRC-1167FSA all versions allow an unauthenticated network-adjacent attacker to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2021-20738**	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRC--190721/461
wrc-1167fsa					
N/A	07-Jul-21	3.3	WRC-1167FS-W, WRC-1167FS-B, and WRC-1167FSA all versions allow an unauthenticated network-adjacent attacker to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2021-20738**	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRC--190721/462
wrc-300febk					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRC--190721/463
wrc-733febk					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRC--190721/464
wrc-f300nf					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRC--190721/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vectors. **CVE ID : CVE-2021-20739**		
wrh-300bk					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRH--190721/466
wrh-300bk-s					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRH--190721/467
wrh-300rd					
Improper Neutralization of Special Elements used in an OS Command ('OS	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRH--190721/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**		
wrh-300sv					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRH--190721/469
wrh-300wh					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRH--190721/470
wrh-300wh-s					
Improper Neutralization of Special	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK,	https://www.elecom.co.jp/news/secu	H-ELE-WRH--190721/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	rity/202107 06-01/	
wrh-h300bk					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRH--190721/472
wrh-h300wh					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	H-ELE-WRH--190721/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Huawei					
hima-l29c					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Jul-21	2.1	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1);	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210630-01-pathtraversal-en	H-HUA-HIMA-190721/474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**		
laya-al00ep					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Jul-21	2.1	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1);	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210630-01-pathtraversal-en	H-HUA-LAYA-190721/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**		
mate_20					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Jul-21	2.1	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16);	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210630-01-pathtraversal-en	H-HUA-MATE-190721/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**		
mate_20_pro					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Jul-21	2.1	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16),	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210630-01-pathtraversal-en	H-HUA-MATE-190721/477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**		
oxfords-an00a					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Jul-21	2.1	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1);	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210630-01-pathtraversal-en	H-HUA-OXFO-190721/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**		
p30					
N/A	13-Jul-21	2.1	The Bluetooth function of some Huawei smartphones has a DoS vulnerability. Attackers can install third-party apps to send specific broadcasts, causing the Bluetooth module to crash. This vulnerability is successfully exploited to cause the Bluetooth function to become abnormal. Affected product versions include: HUAWEI P30 10.0.0.195(C432E22R2P5), 10.0.0.200(C00E85R2P11), 10.0.0.200(C461E6R3P1), 10.0.0.201(C10E7R5P1), 10.0.0.201(C185E4R7P1), 10.0.0.206(C605E19R1P3), 10.0.0.209(C636E6R3P4), 10.0.0.210(C635E3R2P4), and versions earlier than 10.1.0.165(C01E165R2P11). **CVE ID : CVE-2021-22399**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210707-03-dos-en	H-HUA-P30-190721/479
tony-al00b					
Improper Limitation of	13-Jul-21	2.1	There is a path traversal vulnerability in some	https://www.huawei.co	H-HUA-TONY-190721/480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**	m/en/psirt/security-advisories/huawei-sa-20210630-01-pathtraversal-en	
Johnsoncontrols					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c-cure_9000					
Improper Input Validation	01-Jul-21	6.5	An insecure client auto update feature in C-CURE 9000 can allow remote execution of lower privileged Windows programs. **CVE ID : CVE-2021-27660**	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	H-JOH-C-CU-190721/481
f4-snc					
Incorrect Authorization	01-Jul-21	6.5	Successful exploitation of this vulnerability could give an authenticated Facility Explorer SNC Series Supervisory Controller (F4-SNC) user an unintended level of access to the controller's file system, allowing them to access or modify system files by sending specifically crafted web messages to the F4-SNC. **CVE ID : CVE-2021-27661**	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	H-JOH-F4-S-190721/482
jtekt					
2port-efr					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for	N/A	H-JTE-2POR-190721/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
fl\\/et-t-v2h					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	H-JTE-FL\\-190721/484
nano_10gx					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside	N/A	H-JTE-NANO-190721/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
nano_2et					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	H-JTE-NANO-190721/486
nano_cpu					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive	N/A	H-JTE-NANO-190721/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
pc10b					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	H-JTE-PC10-190721/488
pc10b-p					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU,	N/A	H-JTE-PC10-190721/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
pc10e					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	H-JTE-PC10-190721/490
pc10g-cpu					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H,	N/A	H-JTE-PC10-190721/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
pc10ge					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	H-JTE-PC10-190721/492
pc10p					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E,	N/A	H-JTE-PC10-190721/493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
pc10p-dp					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	H-JTE-PC10-190721/494
pc10p-dp-io					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE,	N/A	H-JTE-PC10-190721/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
pc10pe					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	H-JTE-PC10-190721/496
pc10pe-16\\/16p					
Improper Restriction of Operations within the Bounds of a Memory	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano	N/A	H-JTE-PC10-190721/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
plus_2p-efr					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	H-JTE-PLUS-190721/498
plus_bus-ex					
Improper Restriction of Operations within the Bounds of a	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-	N/A	H-JTE-PLUS-190721/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
plus_cpu					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	H-JTE-PLUS-190721/500
plus_efr					
Improper Restriction of Operations within the	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus	N/A	H-JTE-PLUS-190721/501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
plus_efr2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	H-JTE-PLUS-190721/502
plus_ex					
Improper Restriction of Operations	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2,	N/A	H-JTE-PLUS-190721/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
plus_ex2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	H-JTE-PLUS-190721/504
Qualcomm					
apq8009					
Out-of-	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of	https://www.qualcomm.	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	com/company/product-security/bulletins/july-2021-bulletin	190721/505
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/506
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/507
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
apq8009w					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/509
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/510
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
apq8017					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/512
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/513
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/515
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/516
apq8037					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-APQ8-190721/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/518
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/519
Improper Restriction of Operations within the Bounds of a Memory	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-APQ8-190721/520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	bulletin	
apq8053					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/521
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/522
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-APQ8-190721/523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/524
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/525
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1898		
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/527
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/528
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/529
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-APQ8-190721/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/531
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/532
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/533
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/534
apq8064au					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/536
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/537
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/538
Out-of-	13-Jul-21	5	Possible out of bound read	https://ww	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/539
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/540
apq8096au					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/542
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/543
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/545
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-APQ8-190721/546
aqt1000					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause	https://www.qualcomm.com/company/product-	H-QUA-AQT1-190721/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/548
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/549
Improper Restriction of Operations	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in	https://www.qualcomm.com/company/product-	H-QUA-AQT1-190721/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	security/bulletins/july-2021-bulletin	
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/551
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/552
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/553
Out-of-	13-Jul-21	2.1	Possible buffer over read due to lack of length check	https://www.qualcomm.	H-QUA-AQT1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	com/company/product-security/bulletins/july-2021-bulletin	190721/554
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/555
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/556
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/558
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/559
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/561
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/562
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when	https://www.qualcomm.com/compan	H-QUA-AQT1-190721/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/564
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AQT1-190721/565
Improper	13-Jul-21	5	Possible out of bound read	https://ww	H-QUA-AQT1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/566
ar6003					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR60-190721/567
ar7420					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR74-190721/568
ar8031					
Out-of-	13-Jul-21	7.2	Incorrect handling of	https://ww	H-QUA-AR80-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/569
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/570
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/571
Improper	13-Jul-21	7.2	Improper length check of	https://ww	H-QUA-AR80-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/572
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/573
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1938		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/575
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/576
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/578
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/579
ar8035					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-AR80-190721/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/581
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/582
Improper Restriction of Operations within the Bounds of a	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-AR80-190721/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/584
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/585
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-AR80-190721/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/587
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/589
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/590
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR80-190721/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1970		
ar9380					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR93-190721/592
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR93-190721/593
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR93-190721/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1943		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR93-190721/595
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR93-190721/596
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-AR93-190721/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR93-190721/598
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-AR93-190721/599
csr6030					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-CSR6-190721/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	etins/july-2021-bulletin	
csr8811					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSR8-190721/601
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSR8-190721/602
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-CSR8-190721/603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSR8-190721/604
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSR8-190721/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSR8-190721/606
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSR8-190721/607
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSR8-190721/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
csra6620					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/609
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/610
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/612
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/613
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/615
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/616
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/618
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/619
csra6640					
Out-of-	13-Jul-21	7.2	Incorrect handling of	https://ww	H-QUA-CSRA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/620
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/621
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/622
Improper	13-Jul-21	7.2	Improper length check of	https://ww	H-QUA-CSRA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/623
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/624
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1938		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/626
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/627
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/629
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRA-190721/630
csrb31024					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-CSRB-190721/631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRB-190721/632
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRB-190721/633
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-CSRB-190721/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRB-190721/635
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRB-190721/636
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRB-190721/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRB-190721/638
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRB-190721/639
Reachable	13-Jul-21	5	Denial of service in SAP case	https://ww	H-QUA-CSRB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/640
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRB-190721/641
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-CSRB-190721/642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1970		
fsm10055					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/643
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/644
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/646
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/647
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/649
fsm10056					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/650
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/652
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/653
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-FSM1-190721/655
ipq4018					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/656
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/658
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/659
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/661
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/662
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ4-190721/663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	etins/july-2021-bulletin	
ipq4019					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/664
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/665
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/667
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/668
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-IPQ4-190721/669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	bulletin	
ipq4028					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/670
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/671
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/673
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/674
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing	https://www.qualcomm.com/compan	H-QUA-IPQ4-190721/675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/676
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/677
ipq4029					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem	https://www.qualcomm.	H-QUA-IPQ4-190721/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/679
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/680
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	H-QUA-IPQ4-190721/681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/682
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/684
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ4-190721/685
ipq5010					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/687
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/688
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ5-190721/689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/690
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/692
ipq5018					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/693
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/695
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/696
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing	https://www.qualcomm.com/compan	H-QUA-IPQ5-190721/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/698
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/699
ipq5028					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while	https://www.qualcomm.	H-QUA-IPQ5-190721/700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/701
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/703
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/704
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ5-190721/705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ5-190721/706
ipq6000					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/707
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to	https://www.qualcomm.	H-QUA-IPQ6-190721/708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/709
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/711
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/712
ipq6005					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/714
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/715
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while	https://www.qualcomm.com/company/product-	H-QUA-IPQ6-190721/716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/717
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq6010					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/719
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/720
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/722
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/723
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-IPQ6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/724
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/725
ipq6018					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/727
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/728
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/730
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/731
Improper Input	13-Jul-21	10	Possible buffer overflow due to lack of parameter length	https://www.qualcomm.	H-QUA-IPQ6-190721/732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	com/company/product-security/bulletins/july-2021-bulletin	
ipq6028					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/733
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1943		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/735
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/736
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-IPQ6-190721/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/738
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ6-190721/739
ipq8064					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-190721/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/741
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/742
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-IPQ8-190721/743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/744
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/746
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/747
ipq8065					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/748
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-IPQ8-190721/749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/750
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/752
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/753
ipq8068					
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1943		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/755
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/756
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/758
ipq8069					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/759
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1938		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/761
ipq8070					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/762
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-IPQ8-190721/763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/764
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/766
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/767
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
ipq8070a					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/769
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/770
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-190721/771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/772
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/774
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/775
ipq8071					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/777
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/778
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-IPQ8-190721/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/780
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq8071a					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/782
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/783
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/785
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/786
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-IPQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/787
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/788
ipq8072					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/790
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/791
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/793
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/794
ipq8072a					
Reachable	13-Jul-21	5	Possible assertion due to	https://ww	H-QUA-IPQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/795
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/796
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/798
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/799
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-190721/800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/801
ipq8074					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/802
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/804
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/805
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-190721/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/807
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1964**		
ipq8074a					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/809
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/810
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-IPQ8-190721/811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/812
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/814
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/815
ipq8076					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/817
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/818
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-IPQ8-190721/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/820
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/822
ipq8076a					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/823
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/825
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/826
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-190721/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/828
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/829
ipq8078					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	H-QUA-IPQ8-190721/830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/831
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/833
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/834
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-IPQ8-190721/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/836
ipq8078a					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/837
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-IPQ8-190721/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/839
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/841
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/842
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
ipq8173					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/844
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/845
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-IPQ8-190721/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/847
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/849
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/850
ipq8174					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/852
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/853
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-IPQ8-190721/854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/855
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-IPQ8-190721/857
mdm8215					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM8-190721/858
mdm8215m					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM8-190721/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
mdm8615m					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM8-190721/860
mdm9150					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
mdm9205					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/862
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/863
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/865
mdm9206					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/866
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/867
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check	https://www.qualcomm.	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	com/company/product-security/bulletins/july-2021-bulletin	190721/868
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/869
mdm9215					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
mdm9230					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/871
mdm9250					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/872
mdm9310					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of	https://www.qualcomm.	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	com/company/product-security/bulletins/july-2021-bulletin	190721/873
mdm9330					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/874
mdm9607					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-MDM9-190721/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	bulletin	
mdm9615					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/876
mdm9615m					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
mdm9626					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/878
mdm9628					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mdm9630					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/880
mdm9640					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/881
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-MDM9-190721/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/883
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/884
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
mdm9650					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/886
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/887
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in	https://www.qualcomm.com/compan	H-QUA-MDM9-190721/888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	y/product-security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/889
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/890
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when	https://www.qualcomm.com/compan	H-QUA-MDM9-190721/891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	y/product-security/bulletins/july-2021-bulletin	
mdm9655					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/892
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/894
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MDM9-190721/895
msm8909w					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/897
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/898
msm8917					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/900
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/901
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/902
Reachable	13-Jul-21	5	Denial of service in SAP case	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	MSM8-190721/903
msm8920					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/904
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/906
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/907
msm8937					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/909
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/910
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
msm8940					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/912
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/913
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-MSM8-190721/914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/915
msm8953					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/916
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-MSM8-190721/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/918
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/919
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-MSM8-190721/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile **CVE ID : CVE-2021-1907**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/921
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/922
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/924
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/925
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-190721/926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	security/bulletins/july-2021-bulletin	
msm8996au					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/927
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/928
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-190721/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/930
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-MSM8-190721/931
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in	https://www.qualcomm.com/company/product-	H-QUA-MSM8-190721/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	security/bulletins/july-2021-bulletin	
pm8937					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-PM89-190721/933
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-PM89-190721/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-PM89-190721/935
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-PM89-190721/936
pmp8074					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-PMP8-190721/937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-PMP8-190721/938
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-PMP8-190721/939
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-PMP8-190721/940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-PMP8-190721/941
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-PMP8-190721/942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-PMP8-190721/943
qca1062					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA1-190721/944
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA1-190721/945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
qca1064					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA1-190721/946
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA1-190721/947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
qca2062					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA2-190721/948
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA2-190721/949
qca2064					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA2-190721/950
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA2-190721/951
qca2065					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCA2-190721/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA2-190721/953
qca2066					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA2-190721/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA2-190721/955
qca4004					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/957
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/958
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1890		
qca4020					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/960
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/961
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/963
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/964
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca4024					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/966
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/967
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/969
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/970
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-QCA4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/971
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA4-190721/972
qca6164					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/973
qca6174					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to	https://www.qualcomm.com/company/product-	H-QUA-QCA6-190721/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/975
qca6174a					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/976
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-190721/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/978
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/979
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-190721/980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/981
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/982
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/984
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/985
qca6175a					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause	https://www.qualcomm.com/company/product-	H-QUA-QCA6-190721/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/987
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/988
Improper Restriction of Operations	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-190721/989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/990
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/991
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-190721/992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/993
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/995
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/996
qca6234					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/998
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/999
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
qca6310					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1001
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1002
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1938		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1004
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1005
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-190721/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1007
qca6320					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1008
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine	https://www.qualcomm.com/compan	H-QUA-QCA6-190721/1009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1010
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1011
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1013
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1014
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCA6-190721/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1016
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1017
qca6335					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem	https://www.qualcomm.	H-QUA-QCA6-190721/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	com/company/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1019
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1020
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-190721/1021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1022
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1024
qca6390					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1025
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1027
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1028
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1029
Buffer Copy without	13-Jul-21	7.2	Possible buffer overflow due to improper validation of	https://www.qualcomm.	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	com/company/product-security/bulletins/july-2021-bulletin	190721/1030
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1031
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1943		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1033
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1034
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-190721/1035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1036
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1037
Improper	13-Jul-21	10	Possible buffer overflow due	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1038
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1039
qca6391					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1040
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the	https://www.qualcomm.com/compan	H-QUA-QCA6-190721/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1042
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1043
Buffer Copy without Checking Size of Input	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-QCA6-190721/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1045
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1046
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-190721/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1048
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1049
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-190721/1050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1051
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1053
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1054
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6420					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1056
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1057
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1889		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1059
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1060
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1061
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCA6-190721/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1063
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1064
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1065
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCA6-190721/1066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1067
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1068
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-190721/1069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1070
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1072
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1073
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1075
qca6421					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1076
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1078
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1079
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1931		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1081
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1082
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-190721/1083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	security/bulletins/july-2021-bulletin	
qca6426					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1084
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1086
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1087
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1088
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot	https://www.qualcomm.com/company/product-	H-QUA-QCA6-190721/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1090
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1091
Out-of-	13-Jul-21	5	Possible out of bound read	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1092
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1093
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1095
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1096
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCA6-190721/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1098
qca6428					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1099
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1101
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1102
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCA6-190721/1103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1104
qca6430					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1106
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1107
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1109
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1110
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1111
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1112
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images	https://www.qualcomm.com/compan	H-QUA-QCA6-190721/1113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1114
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1115
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-190721/1116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1117
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1118
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-190721/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1120
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1122
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1123
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6431					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1125
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1126
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1889		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1128
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1129
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1131
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1132
qca6436					
Out-of-	13-Jul-21	7.2	Incorrect handling of	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1133
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1134
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1135
Improper	13-Jul-21	7.2	Improper length check of	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1136
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1137
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1138
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-190721/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1140
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1141
Reachable	13-Jul-21	5	Improper handling of	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1142
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1143
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1145
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1146
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCA6-190721/1147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	bulletin	
qca6438					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1148
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1149
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1151
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1152
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	H-QUA-QCA6-190721/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
qca6564					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1154
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1156
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1157
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1158
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of	https://www.qualcomm.	H-QUA-QCA6-190721/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1160
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1162
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1163
qca6564a					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1165
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1166
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1168
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1169
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1170
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of	https://www.qualcomm.	H-QUA-QCA6-190721/1171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1172
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1173
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR	https://www.qualcomm.	H-QUA-QCA6-190721/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1175
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1177
qca6564au					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1178
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCA6-190721/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1180
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1181
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1907		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1183
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1184
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1940		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1186
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1187
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1189
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1190
Improper	13-Jul-21	5	Possible out of bound read	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1191
qca6574					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1192
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1193
Buffer Copy	13-Jul-21	7.2	Possible buffer overflow due	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1194
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1195
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1196
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-190721/1197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1198
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1199
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-190721/1200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1201
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1203
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1204
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1206
qca6574a					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1207
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCA6-190721/1208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1209
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1210
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1907		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1212
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1213
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1940		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1215
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1216
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1218
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1219
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1220
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1221
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1222
qca6574au					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	H-QUA-QCA6-190721/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1224
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1225
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	H-QUA-QCA6-190721/1226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1227
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1228
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1230
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1231
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-190721/1232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1233
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1235
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1236
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1238
qca6584					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1239
qca6584au					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-190721/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1241
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1242
Improper Restriction of Operations within the Bounds of a	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA6-190721/1243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1244
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1245
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1247
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1248
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1250
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1252
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1253
qca6595					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1256
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1258
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1259
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1261
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1262
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1264
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1265
qca6595au					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-190721/1266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	etins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1267
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1268
Improper Restriction of Operations within the	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-190721/1269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1270
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1271
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1273
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1274
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1276
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1277
Reachable	13-Jul-21	5	Denial of service in SAP case	https://ww	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1278
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1279
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1965		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1281
qca6694					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1282
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1284
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1285
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1287
qca6694au					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1288
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1290
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1291
qca6696					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1293
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1294
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1296
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1297
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1299
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1300
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1302
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1303
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-190721/1304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1305
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA6-190721/1306
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in	https://www.qualcomm.com/compan	H-QUA-QCA6-190721/1307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	y/product-security/bulletins/july-2021-bulletin	
qca7500					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA7-190721/1308
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA7-190721/1309
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA7-190721/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA7-190721/1311
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA7-190721/1312
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA7-190721/1313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	etins/july-2021-bulletin	
qca7520					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA7-190721/1314
qca7550					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA7-190721/1315
qca8072					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1317
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1318
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1320
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1321
Improper	13-Jul-21	10	Possible buffer overflow due	https://ww	H-QUA-QCA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1322
qca8075					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1323
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1325
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1326
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA8-190721/1327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1328
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1329
qca8081					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCA8-190721/1330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1331
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1333
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1334
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA8-190721/1335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1336
qca8337					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1337
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA8-190721/1338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1339
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1340
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA8-190721/1341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1342
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1343
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA8-190721/1344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1345
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1347
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA8-190721/1348
qca9367					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1350
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1351
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1352
qca9377					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	H-QUA-QCA9-190721/1353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1354
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1355
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted	https://www.qualcomm.com/compan	H-QUA-QCA9-190721/1356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1357
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1358
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1359
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-190721/1360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1361
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
qca9379					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1363
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1364
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1366
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1367
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca9531					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1369
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1370
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1371
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	H-QUA-QCA9-190721/1372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	com/company/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1373
qca9558					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1374
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while	https://www.qualcomm.com/company/product-	H-QUA-QCA9-190721/1375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1376
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1377
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-QCA9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1378
qca9561					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1379
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1380
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	H-QUA-QCA9-190721/1381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1382
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca9563					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1384
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1385
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1386
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	H-QUA-QCA9-190721/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	com/company/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1388
qca9880					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1389
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while	https://www.qualcomm.com/company/product-	H-QUA-QCA9-190721/1390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1391
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1392
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-QCA9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1393
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1394
qca9882					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1395
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA9-190721/1396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1397
qca9886					
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1398
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	H-QUA-QCA9-190721/1399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1400
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1402
qca9887					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1403
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1404
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	H-QUA-QCA9-190721/1405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1406
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca9888					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1408
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1409
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1411
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1412
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1414
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1415
qca9889					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCA9-190721/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1887	bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1417
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1418
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1420
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1421
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-QCA9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1422
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1423
qca9896					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1424
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCA9-190721/1425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1426
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1427
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	H-QUA-QCA9-190721/1428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
qca9898					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1429
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1430
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-QCA9-190721/1431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1432
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1434
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1435
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
qca9980					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1437
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1438
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1440
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1441
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in	https://www.qualcomm.com/company/product-	H-QUA-QCA9-190721/1442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1443
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1444
qca9982					
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-QCA9-190721/1445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1446
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1448
qca9984					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1449
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1451
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1452
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1454
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1455
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-190721/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	etins/july-2021-bulletin	
qca9985					
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1457
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1458
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in	https://www.qualcomm.com/company/product-	H-QUA-QCA9-190721/1459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1460
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1461
qca9990					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine	https://www.qualcomm.com/compan	H-QUA-QCA9-190721/1462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1463
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1464
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCA9-190721/1465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1466
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1468
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1469
qca9992					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1470
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while	https://www.qualcomm.	H-QUA-QCA9-190721/1471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1472
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1474
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1475
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-190721/1476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1477
qca9994					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1478
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1480
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1481
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA9-190721/1482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1483
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCA9-190721/1485
qcm2290					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM2-190721/1486
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM2-190721/1487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM2-190721/1488
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM2-190721/1489
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM2-190721/1490
Reachable	13-Jul-21	5	Possible assertion due to	https://ww	H-QUA-QCM2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1491
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM2-190721/1492
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM2-190721/1493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM2-190721/1494
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM2-190721/1495
Improper Input	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	H-QUA-QCM2-190721/1496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	com/company/product-security/bulletins/july-2021-bulletin	
qcm4290					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM4-190721/1497
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM4-190721/1498
Buffer Copy without	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in	https://www.qualcomm.	H-QUA-QCM4-190721/1499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	com/company/product-security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM4-190721/1500
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM4-190721/1501
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCM4-190721/1502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM4-190721/1503
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM4-190721/1504
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in	https://www.qualcomm.com/company/product-	H-QUA-QCM4-190721/1505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM4-190721/1506
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM4-190721/1507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM4-190721/1508
qcm6125					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM6-190721/1509
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM6-190721/1510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM6-190721/1511
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM6-190721/1512
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM6-190721/1513
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot	https://www.qualcomm.com/company/product-	H-QUA-QCM6-190721/1514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM6-190721/1515
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM6-190721/1516
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCM6-190721/1517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM6-190721/1518
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM6-190721/1519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM6-190721/1520
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCM6-190721/1521
qcn5021					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1523
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1524
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while	https://www.qualcomm.com/company/product-	H-QUA-QCN5-190721/1525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1526
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1528
qcn5022					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1529
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1531
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1532
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	H-QUA-QCN5-190721/1533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	com/company/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1534
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1535
qcn5024					
Reachable	13-Jul-21	5	An assertion can be reached	https://ww	H-QUA-QCN5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1536
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1537
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1538
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	H-QUA-QCN5-190721/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1540
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1542
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1543
qcn5052					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1545
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1546
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while	https://www.qualcomm.com/company/product-	H-QUA-QCN5-190721/1547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1548
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1550
qcn5054					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1551
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1553
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1554
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1556
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1557
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN5-190721/1558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	etins/july-2021-bulletin	
qcn5064					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1559
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1560
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	H-QUA-QCN5-190721/1561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1562
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
qcn5121					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1564
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1565
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCN5-190721/1566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1567
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1569
qcn5122					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1570
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1572
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1573
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	H-QUA-QCN5-190721/1574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	com/company/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1575
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1576
qcn5124					
Reachable	13-Jul-21	5	Possible assertion due to	https://ww	H-QUA-QCN5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1577
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1578
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1580
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1581
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in	https://www.qualcomm.com/company/product-	H-QUA-QCN5-190721/1582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1583
qcn5152					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1584
Out-of-	13-Jul-21	5	Possible buffer out of bound	https://ww	H-QUA-QCN5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1585
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1586
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1588
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1589
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCN5-190721/1590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	2021-bulletin	
qcn5154					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1591
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1592
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	H-QUA-QCN5-190721/1593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1594
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1596
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1597
qcn5164					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1599
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1600
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN5-190721/1601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1602
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1604
qcn5500					
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1605
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1607
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1608
qcn5501					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1887		
qcn5502					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1610
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1611
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1613
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1614
qcn5550					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1616
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1617
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN5-190721/1618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1619
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN5-190721/1620
qcn6023					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1621
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1622
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1624
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1625
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	H-QUA-QCN6-190721/1626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1627
qcn6024					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1629
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1630
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1632
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1633
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN6-190721/1634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	etins/july-2021-bulletin	
qcn6122					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1635
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1636
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	H-QUA-QCN6-190721/1637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1638
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1640
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN6-190721/1641
qcn7605					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN7-190721/1642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN7-190721/1643
qcn7606					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN7-190721/1644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN7-190721/1645
qcn9000					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1646
Out-of-	13-Jul-21	5	Possible buffer out of bound	https://ww	H-QUA-QCN9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1647
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1648
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1650
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1651
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCN9-190721/1652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	2021-bulletin	
qcn9012					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1653
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1654
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	H-QUA-QCN9-190721/1655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1656
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1658
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1659
qcn9022					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1661
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1662
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN9-190721/1663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1664
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1666
qcn9024					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1667
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1669
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1670
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing	https://www.qualcomm.com/compan	H-QUA-QCN9-190721/1671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1672
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1673
qcn9070					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while	https://www.qualcomm.	H-QUA-QCN9-190721/1674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1675
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1677
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1678
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCN9-190721/1679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1680
qcn9072					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1681
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to	https://www.qualcomm.	H-QUA-QCN9-190721/1682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1683
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1685
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1686
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCN9-190721/1687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	bulletin	
qcn9074					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1688
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1689
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCN9-190721/1690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1691
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1693
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1694
qcn9100					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1696
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1697
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCN9-190721/1698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1699
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCN9-190721/1701
qcs2290					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS2-190721/1702
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS2-190721/1703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS2-190721/1704
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS2-190721/1705
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS2-190721/1706
Reachable	13-Jul-21	5	Possible assertion due to	https://ww	H-QUA-QCS2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1707
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS2-190721/1708
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS2-190721/1709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS2-190721/1710
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS2-190721/1711
Improper Input	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	H-QUA-QCS2-190721/1712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	com/company/product-security/bulletins/july-2021-bulletin	
qcs405					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1713
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1714
Buffer Copy without	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in	https://www.qualcomm.	H-QUA-QCS4-190721/1715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	com/company/product-security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1717
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCS4-190721/1718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	security/bulletins/july-2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1719
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1720
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR	https://www.qualcomm.	H-QUA-QCS4-190721/1721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1722
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**		
qcs410					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1724
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1725
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1727
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1728
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1730
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1731
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
qcs4290					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1733
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1734
Buffer Copy	13-Jul-21	7.2	Possible buffer overflow due	https://ww	H-QUA-QCS4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1735
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1736
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1737
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCS4-190721/1738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1739
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1740
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing	https://www.qualcomm.com/compan	H-QUA-QCS4-190721/1741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1742
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS4-190721/1744
qcs603					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1745
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1747
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1748
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1749
Reachable	13-Jul-21	5	Possible assertion due to	https://ww	H-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1750
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1751
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCS6-190721/1752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	bulletin	
qcs605					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1753
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1754
Buffer Copy without	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in	https://www.qualcomm.	H-QUA-QCS6-190721/1755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	com/company/product-security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1756
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1757
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCS6-190721/1758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1759
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
qcs610					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1761
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1762
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS6-190721/1763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1764
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1765
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-QCS6-190721/1766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1767
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1768
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS6-190721/1769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1770
qcs6125					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1772
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1773
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1774
Buffer Copy	13-Jul-21	5	Possible buffer overflow due	https://ww	H-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1775
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1776
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1777
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in	https://www.qualcomm.com/compan	H-QUA-QCS6-190721/1778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1779
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1781
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1782
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QCS6-190721/1783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**		
qet4101					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QET4-190721/1784
qsm8250					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QSM8-190721/1785
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the	https://www.qualcomm.com/compan	H-QUA-QSM8-190721/1786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QSM8-190721/1787
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QSM8-190721/1788
qsm8350					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	H-QUA-QSM8-190721/1789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QSM8-190721/1790
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QSM8-190721/1791
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	H-QUA-QSM8-190721/1792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QSM8-190721/1793
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QSM8-190721/1794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
qsw8573					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QSW8-190721/1795
qualcomm215					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QUAL-190721/1796
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function	https://www.qualcomm.	H-QUA-QUAL-190721/1797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	com/company/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QUAL-190721/1798
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QUAL-190721/1799
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when	https://www.qualcomm.com/compan	H-QUA-QUAL-190721/1800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QUAL-190721/1801
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QUAL-190721/1802
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-QUAL-190721/1803
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QUAL-190721/1804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	etins/july-2021-bulletin	
sa415m					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1805
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1807
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1808
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1809
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA41-190721/1810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1811
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1812
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA41-190721/1813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1814
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1816
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1817
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA41-190721/1818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**		
sa515m					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1819
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1820
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1822
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1823
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1825
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1826
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1828
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1829
Improper Input	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	H-QUA-SA51-190721/1830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	com/company/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA51-190721/1831
sa6145p					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1832
Double Free	13-Jul-21	7.2	Memory corruption in key	https://ww	H-QUA-SA61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/1833
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1834
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1835
Buffer Copy without	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA	https://www.qualcomm.	H-QUA-SA61-190721/1836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	com/company/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1837
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1838
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SA61-190721/1839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1840
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1841
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while	https://www.qualcomm.com/company/product-	H-QUA-SA61-190721/1842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1843
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1845
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1846
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1970		
sa6150p					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1848
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1849
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1851
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1852
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1853
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	H-QUA-SA61-190721/1854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1855
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1857
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1858
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SA61-190721/1859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1860
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1861
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SA61-190721/1862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	security/bulletins/july-2021-bulletin	
sa6155					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1863
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1864
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SA61-190721/1865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1866
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1867
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1869
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1870
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1872
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1873
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	H-QUA-SA61-190721/1874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1875
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1877
sa6155p					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1878
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1880
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1881
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1882
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while	https://www.qualcomm.com/compan	H-QUA-SA61-190721/1883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1884
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1885
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-SA61-190721/1886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1887
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1889
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1890
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SA61-190721/1891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1892
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA61-190721/1893
sa8145p					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1895
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1896
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1898
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1899
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1901
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1902
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1904
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1906
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1907
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1908
sa8150p					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1909
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1910
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1912
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1913
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1914
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA81-190721/1915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1916
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1918
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1919
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1921
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1922
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SA81-190721/1923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	2021-bulletin	
sa8155					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1924
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1925
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SA81-190721/1926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1927
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1928
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1931		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1930
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1931
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1933
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1934
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in	https://www.qualcomm.com/company/product-	H-QUA-SA81-190721/1935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1936
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1938
sa8155p					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1939
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1941
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1942
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1943
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot	https://www.qualcomm.com/company/product-	H-QUA-SA81-190721/1944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1945
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1946
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while	https://www.qualcomm.com/company/product-	H-QUA-SA81-190721/1947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1948
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1950
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1951
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-SA81-190721/1952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1953
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1954
sa8195p					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1956
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1957
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1960
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1962
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1963
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1965
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1966
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA81-190721/1967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1968
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SA81-190721/1969
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in	https://www.qualcomm.com/compan	H-QUA-SA81-190721/1970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	y/product-security/bulletins/july-2021-bulletin	
sc8180x					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SC81-190721/1971
sc8180x\\+sdx55					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SC81-190721/1972
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SC81-190721/1973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SC81-190721/1974
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SC81-190721/1975
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-SC81-190721/1976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SC81-190721/1977
sc8280xp					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SC82-190721/1978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SC82-190721/1979
sd205					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD20-190721/1980
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD20-190721/1981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD20-190721/1982
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD20-190721/1983
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD20-190721/1984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd210					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD21-190721/1985
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD21-190721/1986
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD21-190721/1987
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD21-190721/1988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD21-190721/1989
sd429					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD42-190721/1990
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD42-190721/1991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD42-190721/1992
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD42-190721/1993
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD42-190721/1994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
sd439					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD43-190721/1995
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD43-190721/1996
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SD43-190721/1997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD43-190721/1998
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD43-190721/1999
sd450					
Out-of-	13-Jul-21	7.2	Incorrect handling of	https://ww	H-QUA-SD45-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/2000
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD45-190721/2001
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD45-190721/2002
Improper	13-Jul-21	7.2	Improper length check of	https://ww	H-QUA-SD45-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/2003
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD45-190721/2004
sd460					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD46-190721/2005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD46-190721/2006
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD46-190721/2007
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD46-190721/2008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD46-190721/2009
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD46-190721/2010
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD46-190721/2011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD46-190721/2012
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD46-190721/2013
Reachable	13-Jul-21	5	Denial of service in SAP case	https://ww	H-QUA-SD46-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/2014
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD46-190721/2015
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD46-190721/2016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1970		
sd480					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD48-190721/2017
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD48-190721/2018
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD48-190721/2019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD48-190721/2020
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD48-190721/2021
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD48-190721/2022
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	H-QUA-SD48-190721/2023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD48-190721/2024
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD48-190721/2025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD48-190721/2026
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD48-190721/2027
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in	https://www.qualcomm.com/company/product-	H-QUA-SD48-190721/2028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD48-190721/2029
sd632					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD63-190721/2030
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the	https://www.qualcomm.com/compan	H-QUA-SD63-190721/2031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD63-190721/2032
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD63-190721/2033
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in	https://www.qualcomm.com/company/product-	H-QUA-SD63-190721/2034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	security/bulletins/july-2021-bulletin	
sd660					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2035
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2037
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2038
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2039
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot	https://www.qualcomm.com/company/product-	H-QUA-SD66-190721/2040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2041
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2042
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while	https://www.qualcomm.com/company/product-	H-QUA-SD66-190721/2043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2044
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2046
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2047
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-SD66-190721/2048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	bulletin	
sd662					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2049
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2050
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-SD66-190721/2051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2052
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2053
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2055
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2056
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while	https://www.qualcomm.com/company/product-	H-QUA-SD66-190721/2057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2058
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2060
sd665					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2061
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2063
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2064
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2066
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2067
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2069
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2070
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2072
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2073
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	H-QUA-SD66-190721/2074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD66-190721/2075
sd670					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2076
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function	https://www.qualcomm.	H-QUA-SD67-190721/2077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	com/company/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2078
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2079
Buffer Copy without Checking	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto,	https://www.qualcomm.com/compan	H-QUA-SD67-190721/2080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2081
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2082
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD67-190721/2083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2084
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2086
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2087
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**		
sd675					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2089
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2090
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2092
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2093
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2094
Out-of-	13-Jul-21	2.1	Possible buffer over read due to lack of length check	https://www.qualcomm.	H-QUA-SD67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	com/company/product-security/bulletins/july-2021-bulletin	190721/2095
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2096
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2097
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2099
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2100
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2102
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2103
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when	https://www.qualcomm.com/compan	H-QUA-SD67-190721/2104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2105
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2106
Improper	13-Jul-21	5	Possible out of bound read	https://ww	H-QUA-SD67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/2107
sd678					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2108
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2109
Buffer Copy	13-Jul-21	7.2	Possible buffer overflow due	https://ww	H-QUA-SD67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/2110
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2111
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2112
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD67-190721/2113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2114
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2115
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2116
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD67-190721/2117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	etins/july-2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2118
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2119
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	H-QUA-SD67-190721/2120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2121
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2123
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2124
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SD67-190721/2125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD67-190721/2126
sd690_5g					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD69-190721/2127
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD69-190721/2128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD69-190721/2129
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD69-190721/2130
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD69-190721/2131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD69-190721/2132
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD69-190721/2133
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SD69-190721/2134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD69-190721/2135
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD69-190721/2136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD69-190721/2137
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD69-190721/2138
sd710					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD71-190721/2139
Buffer Copy	13-Jul-21	7.2	Possible buffer overflow due	https://ww	H-QUA-SD71-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/2140
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD71-190721/2141
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD71-190721/2142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1943		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD71-190721/2143
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD71-190721/2144
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SD71-190721/2145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD71-190721/2146
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD71-190721/2147
sd712					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	H-QUA-SD71-190721/2148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD71-190721/2149
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD71-190721/2150
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	H-QUA-SD71-190721/2151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD71-190721/2152
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD71-190721/2153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
sd720g					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2154
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2155
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-SD72-190721/2156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2157
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2158
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2160
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2161
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2162
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2164
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2165
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2167
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2168
Reachable	13-Jul-21	5	Denial of service in SAP case	https://ww	H-QUA-SD72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/2169
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2170
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1965		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD72-190721/2172
sd730					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2173
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2175
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2176
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2177
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash	https://www.qualcomm.com/compan	H-QUA-SD73-190721/2178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2179
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2180
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2181
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	H-QUA-SD73-190721/2182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2183
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2184
Out-of-	13-Jul-21	5	Possible out of bound read	https://ww	H-QUA-SD73-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/2185
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2186
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2188
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2189
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SD73-190721/2190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD73-190721/2191
sd750g					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD75-190721/2192
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SD75-190721/2193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD75-190721/2194
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD75-190721/2195
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-SD75-190721/2196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD75-190721/2197
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD75-190721/2198
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SD75-190721/2199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD75-190721/2200
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD75-190721/2201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD75-190721/2202
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD75-190721/2203
sd765					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2205
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2206
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2208
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2209
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2211
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2212
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2214
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2216
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2217
sd765g					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2219
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2220
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2222
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2223
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2224
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to	https://www.qualcomm.	H-QUA-SD76-190721/2225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2226
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2228
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2229
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD76-190721/2230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2231
sd768g					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2232
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in	https://www.qualcomm.com/company/product-	H-QUA-SD76-190721/2233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2234
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2235
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD76-190721/2236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2237
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2238
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-SD76-190721/2239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2240
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2242
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2243
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD76-190721/2245
sd778g					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2246
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2248
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2249
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2251
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2252
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2254
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2255
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD77-190721/2256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2257
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2259
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD77-190721/2260
sd780g					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2261
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function	https://www.qualcomm.	H-QUA-SD78-190721/2262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	com/company/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2263
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2264
Buffer Copy without Checking	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto,	https://www.qualcomm.com/compan	H-QUA-SD78-190721/2265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2266
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2267
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD78-190721/2268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2269
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2271
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2272
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2274
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD78-190721/2275
sd7c					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD7C-190721/2276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD7C-190721/2277
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD7C-190721/2278
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD7C-190721/2279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD7C-190721/2280
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD7C-190721/2281
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD7C-190721/2282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
sd820					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD82-190721/2283
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD82-190721/2284
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD82-190721/2285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD82-190721/2286
sd821					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD82-190721/2287
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in	https://www.qualcomm.com/company/product-	H-QUA-SD82-190721/2288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD82-190721/2289
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD82-190721/2290
sd835					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause	https://www.qualcomm.com/company/product-	H-QUA-SD83-190721/2291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD83-190721/2292
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD83-190721/2293
Improper Restriction of Operations	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in	https://www.qualcomm.com/company/product-	H-QUA-SD83-190721/2294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD83-190721/2295
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD83-190721/2296
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD83-190721/2297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD83-190721/2298
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD83-190721/2299
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while	https://www.qualcomm.com/company/product-	H-QUA-SD83-190721/2300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD83-190721/2301
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD83-190721/2302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD83-190721/2303
sd845					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD84-190721/2304
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD84-190721/2305
Reachable	13-Jul-21	5	Possible assertion due to	https://ww	H-QUA-SD84-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/2306
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD84-190721/2307
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD84-190721/2308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD84-190721/2309
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD84-190721/2310
Improper Input	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	H-QUA-SD84-190721/2311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	com/company/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD84-190721/2312
sd850					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2313
Double Free	13-Jul-21	7.2	Memory corruption in key	https://ww	H-QUA-SD85-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/2314
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2315
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2316
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause	https://www.qualcomm.	H-QUA-SD85-190721/2317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2318
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
sd855					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2320
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2321
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2323
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2324
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2325
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer	https://www.qualcomm.com/company/product-	H-QUA-SD85-190721/2326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2327
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2328
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2329
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD85-190721/2330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	etins/july-2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2331
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2332
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	H-QUA-SD85-190721/2333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2334
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2336
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2337
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SD85-190721/2338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD85-190721/2339
sd865_5g					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2340
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2342
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2343
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2345
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2346
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2348
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2349
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD86-190721/2350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2351
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2353
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD86-190721/2354
sd870					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2355
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function	https://www.qualcomm.	H-QUA-SD87-190721/2356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	com/company/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2357
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2358
Buffer Copy without Checking	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto,	https://www.qualcomm.com/compan	H-QUA-SD87-190721/2359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2360
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2361
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD87-190721/2362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2363
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2365
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2366
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2368
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD87-190721/2369
sd888					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2371
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2372
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2374
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2375
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD88-190721/2376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2377
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2378
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in	https://www.qualcomm.com/compan	H-QUA-SD88-190721/2379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	y/product-security/bulletins/july-2021-bulletin	
sd888_5g					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2380
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2381
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in	https://www.qualcomm.com/compan	H-QUA-SD88-190721/2382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	y/product-security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2383
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2384
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2386
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2387
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD88-190721/2388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2389
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2391
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2392
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD88-190721/2394
sda429w					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDA4-190721/2395
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDA4-190721/2396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDA4-190721/2397
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDA4-190721/2398
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDA4-190721/2399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDA4-190721/2400
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDA4-190721/2401
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDA4-190721/2402
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDA4-190721/2403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDA4-190721/2404
sdm429w					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM4-190721/2405
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM4-190721/2406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM4-190721/2407
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM4-190721/2408
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM4-190721/2409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM4-190721/2410
sdm630					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2411
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2413
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2414
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2416
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2417
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2419
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2420
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDM6-190721/2421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2422
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM6-190721/2423
sdm830					
Buffer Copy without	13-Jul-21	7.2	Possible buffer overflow due to improper validation of	https://www.qualcomm.	H-QUA-SDM8-190721/2424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM8-190721/2425
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM8-190721/2426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDM8-190721/2427
sdw2500					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDW2-190721/2428
sdx20					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX2-190721/2429
sdx20m					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX2-190721/2430
sdx24					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDX2-190721/2431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX2-190721/2432
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX2-190721/2433
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDX2-190721/2434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX2-190721/2435
sdx50m					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2436
Double Free	13-Jul-21	7.2	Memory corruption in key	https://ww	H-QUA-SDX5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	190721/2437
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2438
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2439
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of	https://www.qualcomm.	H-QUA-SDX5-190721/2440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2441
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2442
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2443
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot	https://www.qualcomm.com/company/product-	H-QUA-SDX5-190721/2444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2445
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2446
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while	https://www.qualcomm.com/company/product-	H-QUA-SDX5-190721/2447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2448
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2450
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2451
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-SDX5-190721/2452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2453
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2454
sdx55					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2456
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2457
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2459
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2460
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2461
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-SDX5-190721/2462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1899**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2463
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2464
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2465
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-SDX5-190721/2466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2467
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2468
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDX5-190721/2469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2470
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2472
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2473
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2475
sdx55m					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2476
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2478
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2479
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2481
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2482
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2483
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2484
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while	https://www.qualcomm.com/compan	H-QUA-SDX5-190721/2485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2486
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2487
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-SDX5-190721/2488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2489
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2491
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2492
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SDX5-190721/2493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2494
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDX5-190721/2495
sdxr1					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2497
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2498
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2500
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2501
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SDXR-190721/2502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2503
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2505
sdxr2_5g					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2506
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2508
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2509
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-190721/2510
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while	https://www.qualcomm.com/compan	H-QUA-SDXR-190721/2511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-200721/2512
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-200721/2513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-200721/2514
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-200721/2515
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-200721/2516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-200721/2517
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-200721/2518
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE	https://www.qualcomm.com/compan	H-QUA-SDXR-200721/2519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SDXR-200721/2520
sd_455					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_4-200721/2521
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD_4-200721/2522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_4-200721/2523
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_4-200721/2524
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SD_4-200721/2525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_4-200721/2526
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_4-200721/2527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
sd_636					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2528
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2529
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-SD_6-200721/2530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2531
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2532
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2534
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2535
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2537
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2538
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	200721/2539
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2540
sd_675					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2542
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2543
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2544
Out-of-	13-Jul-21	2.1	Possible Buffer Over-read	https://ww	H-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	200721/2545
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2546
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2547
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2548
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while	https://www.qualcomm.com/compan	H-QUA-SD_6-200721/2549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2550
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2551
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-SD_6-200721/2552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2553
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2555
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2556
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SD_6-200721/2557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2558
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_6-200721/2559
sd_8c					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2561
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2562
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2564
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2565
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2567
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2568
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2570
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2571
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in	https://www.qualcomm.com/compan	H-QUA-SD_8-200721/2572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	y/product-security/bulletins/july-2021-bulletin	
sd_8cx					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2573
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2574
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in	https://www.qualcomm.com/compan	H-QUA-SD_8-200721/2575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	y/product-security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2576
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2577
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2579
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2580
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2582
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2584
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SD_8-200721/2585
sm4125					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM41-200721/2586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM41-200721/2587
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM41-200721/2588
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM41-200721/2589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM41-200721/2590
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM41-200721/2591
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM41-200721/2592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM41-200721/2593
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM41-200721/2594
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM41-200721/2595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM41-200721/2596
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM41-200721/2597
sm6250					
Out-of-bounds	13-Jul-21	7.2	Incorrect handling of pointers in trusted	https://www.qualcomm.	H-QUA-SM62-200721/2598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	com/company/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2599
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2600
Improper Restriction	13-Jul-21	7.2	Improper length check of public exponent in RSA	https://www.qualcomm.	H-QUA-SM62-200721/2601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	com/company/product-security/bulletins/july-2021-bulletin	
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2602
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2603
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2605
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2606
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2607
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2609
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2610
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2612
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2613
Reachable	13-Jul-21	5	Denial of service in SAP case	https://ww	H-QUA-SM62-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	200721/2614
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2615
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1965		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2617
sm6250p					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2618
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2620
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2621
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2622
Reachable	13-Jul-21	5	Possible assertion due to	https://ww	H-QUA-SM62-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	200721/2623
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2624
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2626
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM62-200721/2627
sm7250p					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2629
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2630
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2632
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2633
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2635
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2636
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2638
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2640
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM72-200721/2641
sm7315					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2642
Buffer Copy without	13-Jul-21	7.2	Possible buffer overflow due to improper validation of	https://www.qualcomm.	H-QUA-SM73-200721/2643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2644
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1943		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2646
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2647
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SM73-200721/2648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2649
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2650
Improper	13-Jul-21	10	Possible buffer overflow due	https://ww	H-QUA-SM73-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	200721/2651
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2652
sm7325p					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2653
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the	https://www.qualcomm.com/compan	H-QUA-SM73-200721/2654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2655
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2656
Buffer Copy without Checking Size of Input	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-SM73-200721/2657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2658
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2659
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SM73-200721/2660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2661
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2663
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2664
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2666
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-SM73-200721/2667
wcd9306					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2669
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2670
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
wcd9326					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2672
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2673
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2674
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCD9-200721/2675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2676
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2677
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1938		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2679
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2680
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2682
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2683
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCD9-200721/2684
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2685
wcd9330					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2686
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-WCD9-200721/2687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2688
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2689
wcd9335					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCD9-200721/2690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2691
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2692
Improper Restriction of Operations within the Bounds of a Memory	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCD9-200721/2693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2694
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2695
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2697
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2698
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2700
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2701
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCD9-200721/2702
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2703
wcd9340					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2704
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCD9-200721/2705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2706
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2707
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2708
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCD9-200721/2709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2710
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2711
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCD9-200721/2712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2713
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2715
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2716
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1970		
wcd9341					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2718
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2719
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2720
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2722
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2723
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2724
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2726
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2727
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCD9-200721/2728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2729
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2731
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2732
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1965		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2734
wcd9360					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2735
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2737
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2738
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2740
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2741
wcd9370					
Out-of-	13-Jul-21	7.2	Incorrect handling of	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCD9-200721/2742
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2743
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2744
Improper	13-Jul-21	7.2	Improper length check of	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCD9-200721/2745
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2746
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2747
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCD9-200721/2748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1899	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2749
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2750
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2751
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2753
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2754
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCD9-200721/2755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2756
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2758
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2759
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2761
wcd9371					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2762
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2764
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2765
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1931		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2767
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2768
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2770
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2771
wcd9375					
Out-of-	13-Jul-21	7.2	Incorrect handling of	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCD9-200721/2772
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2773
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2774
Improper	13-Jul-21	7.2	Improper length check of	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCD9-200721/2775
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2776
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2777
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCD9-200721/2778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1899	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2779
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2780
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2781
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2783
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2784
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCD9-200721/2785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2786
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2788
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2789
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2791
wcd9380					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2792
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2794
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2795
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2797
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2798
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2799
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2800
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while	https://www.qualcomm.com/compan	H-QUA-WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	y/product-security/bulletins/july-2021-bulletin	200721/2801
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2802
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2803
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	H-QUA-WCD9-200721/2804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2805
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2807
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2808
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCD9-200721/2809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2810
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2811
wcd9385					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2813
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2814
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2816
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2817
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2819
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2820
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2822
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2824
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2825
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCD9-200721/2826
wcn3610					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2827
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2828
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2830
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2831
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2832
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCN3-200721/2833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1899**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2834
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2835
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wcn3615					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2837
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2838
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1889		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2840
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2841
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2842
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-200721/2843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2844
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2845
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2846
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-WCN3-200721/2847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2848
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2850
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2851
wcn3620					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2853
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2854
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1890		
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2856
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2857
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2858
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2860
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2861
wcn3660					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2863
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2864
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1890**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2866
wcn3660b					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2867
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCN3-200721/2868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2869
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2870
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCN3-200721/2871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2872
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2873
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2874
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1940**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2876
wcn3680					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2877
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCN3-200721/2878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2879
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2880
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCN3-200721/2881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2882
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2883
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2884
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
wcn3680b					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2886
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2887
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-WCN3-200721/2888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2889
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2890
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1898**		
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2892
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2893
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2894
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2896
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2897
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2899
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2900
wcn3910					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-200721/2901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	etins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2902
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2903
Improper Restriction of Operations within the	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-200721/2904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2905
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2906
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2908
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2909
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-200721/2910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2911
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2913
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2914
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wcn3950					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2916
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2917
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1889		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2919
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2920
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2921
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-200721/2922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2923
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2924
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2925
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCN3-200721/2926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2927
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2928
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-WCN3-200721/2929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2930
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2932
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2933
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCN3-200721/2934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2935
wcn3980					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2936
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2937
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check	https://www.qualcomm.	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	com/company/product-security/bulletins/july-2021-bulletin	200721/2938
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2939
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2940
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2941
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	200721/2942
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2943
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2944
Out-of-	13-Jul-21	5	Possible out of bound read	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN3-200721/2945
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2946
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2948
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2949
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-WCN3-200721/2950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2951
wcn3988					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2952
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCN3-200721/2953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2954
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2955
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCN3-200721/2956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2957
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2958
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1907		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2961
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2962
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1940		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2964
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2965
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2967
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2968
Improper	13-Jul-21	5	Possible buffer over read	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN3-200721/2969
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2970
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2971
wcn3990					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted	https://www.qualcomm.com/compan	H-QUA-WCN3-200721/2972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2973
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2974
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2976
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2977
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2979
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2980
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in	https://www.qualcomm.com/company/product-	H-QUA-WCN3-200721/2981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2982
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2983
wcn3991					
Out-of-	13-Jul-21	7.2	Incorrect handling of	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN3-200721/2984
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2985
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2986
Improper	13-Jul-21	7.2	Improper length check of	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN3-200721/2987
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2988
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2989
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1898		
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2991
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2992
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2993
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1931		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2995
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2996
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2998
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/2999
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in	https://www.qualcomm.com/company/product-	H-QUA-WCN3-200721/3000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3001
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3003
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3004
wcn3998					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3006
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3007
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3008
N/A	13-Jul-21	3.3	Weak configuration in	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN3-200721/3009
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3010
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3011
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3012
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer	https://www.qualcomm.com/company/product-	H-QUA-WCN3-200721/3013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3014
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3015
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3017
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3018
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3020
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3021
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in	https://www.qualcomm.com/company/product-	H-QUA-WCN3-200721/3022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3023
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3024
Improper Input	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	com/company/product-security/bulletins/july-2021-bulletin	200721/3025
wcn3999					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3026
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3027
Buffer Copy without	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in	https://www.qualcomm.	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	com/company/product-security/bulletins/july-2021-bulletin	200721/3028
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3029
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3030
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-WCN3-200721/3031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	security/bulletins/july-2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3032
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3033
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR	https://www.qualcomm.	H-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	com/company/product-security/bulletins/july-2021-bulletin	200721/3034
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3035
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN3-200721/3036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**		
wcn6740					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3037
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3038
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3040
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3041
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3043
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3044
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3046
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3047
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when	https://www.qualcomm.com/compan	H-QUA-WCN6-200721/3048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3049
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3050
Improper	13-Jul-21	5	Possible out of bound read	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN6-200721/3051
wcn6745					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3052
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
wcn6750					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3054
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3055
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN6-200721/3056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3057
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3058
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3060
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3061
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCN6-200721/3062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3063
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3065
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3066
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1965		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3068
wcn6850					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3069
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3071
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3072
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3073
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN6-200721/3074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3075
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3076
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCN6-200721/3077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3078
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3080
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3081
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3083
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3084
wcn6851					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3086
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3087
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1890		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3089
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3090
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3091
Out-of-	13-Jul-21	5	Possible buffer out of bound	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN6-200721/3092
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3093
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3095
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3096
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in	https://www.qualcomm.com/company/product-	H-QUA-WCN6-200721/3097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3098
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3099
wcn6855					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCN6-200721/3100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3101
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3102
Improper Restriction of Operations within the Bounds of a	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCN6-200721/3103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3104
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3105
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WCN6-200721/3106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3107
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3108
Improper	13-Jul-21	5	Possible out of bound read	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN6-200721/3109
wcn6856					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3110
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3111
Buffer Copy	13-Jul-21	7.2	Possible buffer overflow due	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN6-200721/3112
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3113
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3114
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCN6-200721/3115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3116
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3117
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	H-QUA-WCN6-200721/3118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3119
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3121
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3122
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WCN6-200721/3123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WCN6-200721/3124
whs9410					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WHS9-200721/3125
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WHS9-200721/3126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	2021-bulletin	
wsa8810					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3127
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3128
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1898**		
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3130
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3131
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3132
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3134
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3135
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3137
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3138
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing	https://www.qualcomm.com/compan	H-QUA-WSA8-200721/3139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3140
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3142
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3143
wsa8815					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3144
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-WSA8-200721/3145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3146
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3147
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3148
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WSA8-200721/3149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile **CVE ID : CVE-2021-1907**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3150
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3151
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1940**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3153
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3154
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3156
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3158
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3159
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3160
wsa8830					
Out-of-bounds	13-Jul-21	7.2	Incorrect handling of pointers in trusted	https://www.qualcomm.	H-QUA-WSA8-200721/3161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	com/company/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3162
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3163
Improper Restriction	13-Jul-21	7.2	Improper length check of public exponent in RSA	https://www.qualcomm.	H-QUA-WSA8-200721/3164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	com/company/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3165
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3166
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	H-QUA-WSA8-200721/3167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3168
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3169
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR	https://www.qualcomm.	H-QUA-WSA8-200721/3170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3171
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3173
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3174
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**		
wsa8835					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3176
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3177
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3179
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3180
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3182
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3183
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3185
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3186
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when	https://www.qualcomm.com/compan	H-QUA-WSA8-200721/3187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3188
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	H-QUA-WSA8-200721/3189
Improper	13-Jul-21	5	Possible out of bound read	https://ww	H-QUA-WSA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	200721/3190
Rockwellautomation					
micrologix_1100					
N/A	09-Jul-21	5	Rockwell Automation MicroLogix 1100, all versions, allows a remote, unauthenticated attacker sending specially crafted commands to cause the PLC to fault when the controller is switched to RUN mode, which results in a denial-of-service condition. If successfully exploited, this vulnerability will cause the controller to fault whenever the controller is switched to RUN mode. **CVE ID : CVE-2021-33012**	N/A	H-ROC-MICR-200721/3191
tieline					
ip_audtio_gateway					
Incorrect Authorization	01-Jul-21	7.5	Tieline IP Audio Gateway 2.6.4.8 and below is affected by Incorrect Access Control. A vulnerability in the Tieline Web Administrative Interface could allow an unauthenticated user to access a sensitive part of the	N/A	H-TIE-IP_A-200721/3192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system with a high privileged account. **CVE ID : CVE-2021-35336**		
Zyxel					
usg100					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG1-200721/3193
usg1000					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG1-200721/3194
usg110					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35	https://www.zyxel.com/support/Zyxel_security_advisory_for_a	H-ZYX-USG1-200721/3195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	ttacks_against_security_appliances.shtml	
usg1100					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG1-200721/3196
usg1900					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG1-200721/3197
usg20					
Improper	02-Jul-21	7.5	An authentication bypasss	https://ww	H-ZYX-USG2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	w.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	200721/3198
usg20-vpn					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG2-200721/3199
usg200					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device.	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG2-200721/3200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35029		
usg2000					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG2-200721/3201
usg20w					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG2-200721/3202
usg20w-vpn					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.sht	H-ZYX-USG2-200721/3203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	ml	
usg210					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG2-200721/3204
usg2200-vpn					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG2-200721/3205
usg300					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series	https://www.zyxel.com/support/Zyxel_security_a	H-ZYX-USG3-200721/3206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	dvisory_for_attacks_against_security_appliances.shtml	
usg310					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG3-200721/3207
usg40					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG4-200721/3208
usg40w					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG4-200721/3209
Usg50					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG5-200721/3210
usg60					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG6-200721/3211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on an affected device. **CVE ID : CVE-2021-35029**		
usg60w					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG6-200721/3212
usg_flex_100					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG_-200721/3213
usg_flex_100w					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_ap	H-ZYX-USG_-200721/3214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	pliances.shtml	
usg_flex_200					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG_-200721/3215
usg_flex_500					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-USG_-200721/3216
usg_flex_700					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface	https://www.zyxel.com/support/Zyx	H-ZYX-USG_-200721/3217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	el_security_advisory_for_attacks_against_security_appliances.shtml	
zywall_110					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-ZYWA-200721/3218
zywall_1100					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-ZYWA-200721/3219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
zywall_310					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-ZYWA-200721/3220
zywall_atp100					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-ZYWA-200721/3221
zywall_atp100w					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-ZYWA-200721/3222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**		
zywall_atp200					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-ZYWA-200721/3223
zywall_atp500					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-ZYWA-200721/3224
zywall_atp700					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex,	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_agains	H-ZYX-ZYWA-200721/3225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	t_security_appliances.shtml	
zywall_atp800					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-ZYWA-200721/3226
zywall_vpn100					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-ZYWA-200721/3227
zywall_vpn300					
Improper Authenticati	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-	https://www.zyxel.com/	H-ZYX-ZYWA-200721/3228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	
zywall_vpn50					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	H-ZYX-ZYWA-200721/3229
Operating System					
a-stage-inc					
at-40cm01sr_firmware					
Improper Authentication	07-Jul-21	7.5	Improper authentication vulnerability in SCT-40CM01SR and AT-40CM01SR allows an attacker to bypass access restriction and execute an arbitrary command via telnet. **CVE ID : CVE-2021-20776**	N/A	O-A-S-AT-4-220721/3230
sct-40cm01sr_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Jul-21	7.5	Improper authentication vulnerability in SCT-40CM01SR and AT-40CM01SR allows an attacker to bypass access restriction and execute an arbitrary command via telnet. **CVE ID : CVE-2021-20776**	N/A	O-A-S-SCT--220721/3231
Cisco					
asyncos					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Jul-21	9	A vulnerability in the configuration management of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to perform command injection and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied XML input for the web interface. An attacker could exploit this vulnerability by uploading crafted XML configuration files that contain scripting code to a vulnerable device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root. An attacker would need a valid user account with the rights to upload configuration files to exploit this vulnerability.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-scr-web-priv-esc-k3HCGJZ	O-CIS-ASYN-220721/3232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1359		
video_surveillance_7070_firmware					
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1595**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	O-CIS-VIDE-220721/3233
Missing Release of Memory	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP)	https://tools.cisco.com/security/center	O-CIS-VIDE-220721/3234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1596**	/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-	O-CIS-VIDE-220721/3235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1597**	wGqundTq	
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	O-CIS-VIDE-220721/3236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1598**		
video_surveillance_7530pd_firmware					
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	O-CIS-VIDE-220721/3237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1595**		
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	O-CIS-VIDE-220721/3238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1596**		
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	O-CIS-VIDE-220721/3239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1597**		
Missing Release of Memory after Effective Lifetime	08-Jul-21	3.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcamera-lldp-mem-wGqundTq	O-CIS-VIDE-220721/3240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1598**		
elecom					
wrc-1167fs-b_firmware					
N/A	07-Jul-21	3.3	WRC-1167FS-W, WRC-1167FS-B, and WRC-1167FSA all versions allow an unauthenticated network-adjacent attacker to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2021-20738**	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRC--220721/3241
wrc-1167fs-w_firmware					
N/A	07-Jul-21	3.3	WRC-1167FS-W, WRC-1167FS-B, and WRC-1167FSA all versions allow an unauthenticated network-adjacent attacker to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2021-20738**	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRC--220721/3242
wrc-1167fsa_firmware					
N/A	07-Jul-21	3.3	WRC-1167FS-W, WRC-1167FS-B, and WRC-1167FSA all versions allow an unauthenticated network-adjacent attacker to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2021-20738**	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRC--220721/3243
wrc-300febk_firmware					
Improper Neutralization of Special Elements used in an OS	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRC--220721/3244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**		
wrc-733febk_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRC--220721/3245
wrc-f300nf_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRC--220721/3246
wrh-300bk-s_firmware					
Improper	07-Jul-21	5.8	WRC-300FEBK, WRC-	https://ww	O-ELE-WRH--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	w.elecom.co.jp/news/security/20210706-01/	220721/3247
wrh-300bk_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRH--220721/3248
wrh-300rd_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors.	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRH--220721/3249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20739		
wrh-300sv_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRH--220721/3250
wrh-300wh-s_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRH--220721/3251
wrh-300wh_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRH--220721/3252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**		
wrh-h300bk_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRH--220721/3253
wrh-h300wh_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Jul-21	5.8	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors. **CVE ID : CVE-2021-20739**	https://www.elecom.co.jp/news/security/20210706-01/	O-ELE-WRH--220721/3254
Fedoraproject					
fedora					
Improper Restriction of	09-Jul-21	8	A flaw was found in the ptp4l program of the linuxptp package. A missing	https://bugzilla.redhat.com/show_bug	O-FED-FEDO-220721/3255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			length check when forwarding a PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before 2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1. **CVE ID : CVE-2021-3570**	.cgi?id=1966240	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-21	7.2	An out-of-bounds memory write flaw was found in the Linux kernel's joystick devices subsystem in versions before 5.9-rc1, in the way the user calls ioctl JSIOCSBTNMAP. This flaw allows a local user to crash the system or possibly escalate their privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2021-3612**	https://lore.kernel.org/linux-input/20210620120030.1513655-1-avlarkin82@gmail.com/	O-FED-FEDO-220721/3256
Google					
android					
Incorrect Default Permissions	14-Jul-21	4.4	In onCreate of PermissionActivity.java, there is a possible permission bypass due to	https://source.android.com/security/bulletin/202	O-GOO-ANDR-220721/3257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Confusing UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174495520 **CVE ID : CVE-2021-0441**	1-07-01	
Incorrect Default Permissions	14-Jul-21	4.6	In onPackageAddedInternal of PermissionManagerService.java, there is possible access to external storage due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-171430330 **CVE ID : CVE-2021-0486**	https://source.android.com/security/bulletin/2021-07-01	O-GOO-ANDR-220721/3258
Missing Authorization	14-Jul-21	4.9	In notifyProfileAdded and notifyProfileRemoved of SipService.java, there is a possible way to retrieve SIP account names due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-	https://source.android.com/security/bulletin/2021-07-01	O-GOO-ANDR-220721/3259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			176496502 **CVE ID : CVE-2021-0597**		
Exposure of Sensitive Information to an Unauthorized Actor	08-Jul-21	5	Improper component protection vulnerability in SmsViewerActivity of Samsung Message prior to SMR July-2021 Release 1 allows untrusted applications to access Message files. **CVE ID : CVE-2021-25426**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=7	O-GOO-ANDR-220721/3260
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jul-21	3.3	SQL injection vulnerability in Bluetooth prior to SMR July-2021 Release 1 allows unauthorized access to paired device information **CVE ID : CVE-2021-25427**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=7	O-GOO-ANDR-220721/3261
Improper Input Validation	08-Jul-21	4.6	Improper validation check vulnerability in PackageManager prior to SMR July-2021 Release 1 allows untrusted applications to get dangerous level permission without user confirmation in limited circumstances. **CVE ID : CVE-2021-25428**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=7	O-GOO-ANDR-220721/3262
Improper Privilege Management	08-Jul-21	3.3	Improper privilege management vulnerability in Bluetooth application prior to SMR July-2021 Release 1 allows untrusted application to access the Bluetooth information in Bluetooth application.	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=7	O-GOO-ANDR-220721/3263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25429		
Improper Authentication	08-Jul-21	3.3	Improper access control vulnerability in Bluetooth application prior to SMR July-2021 Release 1 allows untrusted application to access the Bluetooth information in Bluetooth application. **CVE ID : CVE-2021-25430**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=7	O-GOO-ANDR-220721/3264
Incorrect Authorization	08-Jul-21	2.1	Improper access control vulnerability in Cameralyzer prior to versions 3.2.1041 in 3.2.x, 3.3.1040 in 3.3.x, and 3.4.4210 in 3.4.x allows untrusted applications to access some functions of Cameralyzer. **CVE ID : CVE-2021-25431**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	O-GOO-ANDR-220721/3265
Exposure of Resource to Wrong Sphere	08-Jul-21	2.1	Information exposure vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to access chat data. **CVE ID : CVE-2021-25432**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	O-GOO-ANDR-220721/3266
Externally Controlled Reference to a Resource in Another Sphere	14-Jul-21	4.9	In scheduleTimeoutLocked of NotificationRecord.java, there is a possible disclosure of a sensitive identifier via broadcasted intent due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not	https://source.android.com/security/bulletin/2021-07-01	O-GOO-ANDR-220721/3267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-175614289 **CVE ID : CVE-2021-0599**		
Incorrect Authorization	08-Jul-21	4.6	Improper access control vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to cause local file inclusion in webview. **CVE ID : CVE-2021-25438**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	O-GOO-ANDR-220721/3268
Incorrect Authorization	08-Jul-21	2.1	Improper access control vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to cause arbitrary webpage loading in webview. **CVE ID : CVE-2021-25439**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	O-GOO-ANDR-220721/3269
Improper Input Validation	08-Jul-21	4.6	Improper input validation vulnerability in AR Emoji Editor prior to version 4.4.03.5 in Android Q(10.0) and above allows untrusted applications to access arbitrary files with an escalated privilege. **CVE ID : CVE-2021-25441**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	O-GOO-ANDR-220721/3270
Improper Input	14-Jul-21	6.9	In onCreate of DeviceAdminAdd.java, there	https://source.android.co	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			is a possible way to mislead a user to activate a device admin app due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-179042963 **CVE ID : CVE-2021-0600**	m/security/bulletin/2021-07-01	220721/3271
Out-of-bounds Write	14-Jul-21	4.9	In encodeFrames of avc_enc_fuzzer.cpp, there is a possible out of bounds write due to a double free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-180643802 **CVE ID : CVE-2021-0601**	https://source.android.com/security/bulletin/2021-07-01	O-GOO-ANDR-220721/3272
Improper Privilege Management	14-Jul-21	7.2	In onCreateOptionsMenu of WifiNetworkDetailsFragment.java, there is a possible way for guest users to view and modify Wi-Fi settings for all configured APs due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User	https://source.android.com/security/bulletin/2021-07-01	O-GOO-ANDR-220721/3273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-177573895 **CVE ID : CVE-2021-0602**		
Huawei					
emui					
N/A	01-Jul-21	6.4	There is a Configuration Defect vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service integrity and availability. **CVE ID : CVE-2021-22343**	https://consumer.huawei.com/en/support/bulletin/2021/5/	O-HUA-EMUI-220721/3274
N/A	01-Jul-21	5	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause temporary DoS. **CVE ID : CVE-2021-22344**	https://consumer.huawei.com/en/support/bulletin/2021/5/	O-HUA-EMUI-220721/3275
N/A	01-Jul-21	5	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause temporary DoS. **CVE ID : CVE-2021-22347**	https://consumer.huawei.com/en/support/bulletin/2021/5/	O-HUA-EMUI-220721/3276
harmonyos					
NULL Pointer Dereference	14-Jul-21	4.9	A component of the HarmonyOS 2.0 has a Null Pointer Dereference Vulnerability. Local attackers may exploit this vulnerability to cause	N/A	O-HUA-HARM-220721/3277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system denial of service. **CVE ID : CVE-2021-22318**		
hima-l29c_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Jul-21	2.1	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210630-01-pathtraversal-en	O-HUA-HIMA-220721/3278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**		
laya-al00ep_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Jul-21	2.1	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210630-01-pathtraversal-en	O-HUA-LAYA-220721/3279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**		
magic_ui					
N/A	01-Jul-21	6.4	There is a Configuration Defect vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service integrity and availability. **CVE ID : CVE-2021-22343**	https://consumer.huawei.com/en/support/bulletin/2021/5/	O-HUA-MAGI-220721/3280
N/A	01-Jul-21	5	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause temporary DoS. **CVE ID : CVE-2021-22344**	https://consumer.huawei.com/en/support/bulletin/2021/5/	O-HUA-MAGI-220721/3281
N/A	01-Jul-21	5	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause temporary DoS. **CVE ID : CVE-2021-22347**	https://consumer.huawei.com/en/support/bulletin/2021/5/	O-HUA-MAGI-220721/3282
mate_20_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Jul-21	2.1	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210630-01-	O-HUA-MATE-220721/3283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**	pathtraversal-en	
mate_20_pro_firmware					
Improper Limitation of a Pathname to a Restricted Directory	13-Jul-21	2.1	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-	O-HUA-MATE-220721/3284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**	20210630-01-pathtraversal-en	
oxfords-an00a_firmware					
Improper Limitation of a Pathname to a	13-Jul-21	2.1	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that	https://www.huawei.com/en/psirt/security-	O-HUA-OXFO-220721/3285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**	advisories/huawei-sa-20210630-01-pathtraversal-en	
p30_firmware					
N/A	13-Jul-21	2.1	The Bluetooth function of some Huawei smartphones	https://www.huawei.co	O-HUA-P30_-220721/3286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has a DoS vulnerability. Attackers can install third-party apps to send specific broadcasts, causing the Bluetooth module to crash. This vulnerability is successfully exploited to cause the Bluetooth function to become abnormal. Affected product versions include: HUAWEI P30 10.0.0.195(C432E22R2P5), 10.0.0.200(C00E85R2P11), 10.0.0.200(C461E6R3P1), 10.0.0.201(C10E7R5P1), 10.0.0.201(C185E4R7P1), 10.0.0.206(C605E19R1P3), 10.0.0.209(C636E6R3P4), 10.0.0.210(C635E3R2P4), and versions earlier than 10.1.0.165(C01E165R2P11). **CVE ID : CVE-2021-22399**	m/en/psirt/security-advisories/huawei-sa-20210707-03-dos-en	
tony-al00b_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Jul-21	2.1	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210630-01-pathtraversal-en	O-HUA-TONY-220721/3287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1). **CVE ID : CVE-2021-22440**		
IBM					
aix					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-21	4.3	IBM InfoSphere Information Server 11.7 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: 200966. **CVE ID : CVE-2021-29712**	https://www.ibm.com/support/pages/node/6468581, https://exchange.xforce.ibmcloud.com/vulnerabilities/200966	O-IBM-AIX-220721/3288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Johnsoncontrols					
c-cure_9000_firmware					
Improper Input Validation	01-Jul-21	6.5	An insecure client auto update feature in C-CURE 9000 can allow remote execution of lower privileged Windows programs. **CVE ID : CVE-2021-27660**	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	O-JOH-C-CU-220721/3289
f4-snc_firmware					
Incorrect Authorization	01-Jul-21	6.5	Successful exploitation of this vulnerability could give an authenticated Facility Explorer SNC Series Supervisory Controller (F4-SNC) user an unintended level of access to the controller's file system, allowing them to access or modify system files by sending specifically crafted web messages to the F4-SNC. **CVE ID : CVE-2021-27661**	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	O-JOH-F4-S-220721/3290
jtekt					
2port-efr_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside	N/A	O-JTE-2POR-220721/3291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
fl\\/et-t-v2h_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	O-JTE-FL\\-220721/3292
nano_10gx_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive	N/A	O-JTE-NANO-220721/3293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
nano_2et_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	O-JTE-NANO-220721/3294
nano_cpu_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU,	N/A	O-JTE-NANO-220721/3295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
pc10b-p_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	O-JTE-PC10-220721/3296
pc10b_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H,	N/A	O-JTE-PC10-220721/3297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
pc10e_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	O-JTE-PC10-220721/3298
pc10g-cpu_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E,	N/A	O-JTE-PC10-220721/3299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
pc10ge_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	O-JTE-PC10-220721/3300
pc10p-dp-io_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE,	N/A	O-JTE-PC10-220721/3301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
pc10p-dp_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	O-JTE-PC10-220721/3302
pc10pe-16\\/16p_firmware					
Improper Restriction of Operations within the Bounds of a Memory	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano	N/A	O-JTE-PC10-220721/3303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
pc10pe_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	O-JTE-PC10-220721/3304
pc10p_firmware					
Improper Restriction of Operations within the Bounds of a	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-	N/A	O-JTE-PC10-220721/3305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
plus_2p-efr_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	O-JTE-PLUS-220721/3306
plus_bus-ex_firmware					
Improper Restriction of Operations within the	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus	N/A	O-JTE-PLUS-220721/3307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
plus_cpu_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	O-JTE-PLUS-220721/3308
plus_efr2_firmware					
Improper Restriction of Operations	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2,	N/A	O-JTE-PLUS-220721/3309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
plus_efr_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	O-JTE-PLUS-220721/3310
plus_ex2_firmware					
Improper Restriction of	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR,	N/A	O-JTE-PLUS-220721/3311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**		
plus_ex_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Jul-21	7.8	When JTEKT Corporation TOYOPUC PLC versions PC10G-CPU, 2PORT-EFR, Plus CPU, Plus EX, Plus EX2, Plus EFR, Plus EFR2, Plus 2P-EFR, PC10P-DP, PC10P-DP-IO, Plus BUS-EX, Nano 10GX, Nano 2ET,PC10PE, PC10PE-16/16P, PC10E, FL/ET-T-V2H, PC10B,PC10B-P, Nano CPU, PC10P, and PC10GE receive an invalid frame, the outside area of a receive buffer for FL-net are overwritten. As a result, the PLC CPU detects a system error, and the affected products stop. **CVE ID : CVE-2021-27477**	N/A	O-JTE-PLUS-220721/3312
Linux					
acrn					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jul-21	5	ACRN before 2.5 has a hw/pci/virtio/virtio.c vq_endchains NULL Pointer Dereference. **CVE ID : CVE-2021-36143**	https://github.com/projectacrn/acrn-hypervisor/commit/154fe59531c12b82e26d1b24b5531f5066d224f5	O-LIN-ACRN-220721/3313
Use After Free	02-Jul-21	5	The polling timer handler in ACRN before 2.5 has a use-after-free for a freed virtio device, related to devicemodel/hw/pci/virtio/*.c. **CVE ID : CVE-2021-36144**	https://github.com/projectacrn/acrn-hypervisor/pull/6268/commits/dd88504804e186029f845a166dc5c31695e2cca2	O-LIN-ACRN-220721/3314
Use After Free	02-Jul-21	5	The Device Model in ACRN through 2.5 has a devicemodel/core/mem.c use-after-free for a freed rb_entry. **CVE ID : CVE-2021-36145**	https://github.com/projectacrn/acrn-hypervisor/pull/6058/commits/f880086ffe5423e67d968c8f8f665954786582ce	O-LIN-ACRN-220721/3315
NULL Pointer Dereference	02-Jul-21	5	ACRN before 2.5 has a devicemodel/hw/pci/xhci.c NULL Pointer Dereference for a trb pointer. **CVE ID : CVE-2021-36146**	https://github.com/projectacrn/acrn-hypervisor/pull/6173/commits/330359921e2e4c2f3f3a10b5bab86942d63c4428	O-LIN-ACRN-220721/3316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jul-21	5	An issue was discovered in ACRN before 2.5. It allows a devicemodel/hw/pci/virtio/virtio_net.c virtio_net_ping_rxq NULL pointer dereference for vq->used. **CVE ID : CVE-2021-36147**	https://github.com/projectacrn/acrn-hypervisor/pull/6121/commits/131116b15b0e35a62085d23686b43ed1c12c1331	O-LIN-ACRN-220721/3317
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jul-21	6.8	An issue was discovered in ACRN before 2.5. dmar_free_irte in hypervisor/arch/x86/vtd.c allows an irte_alloc_bitmap buffer overflow. **CVE ID : CVE-2021-36148**	https://github.com/projectacrn/acrn-hypervisor/commit/25c0e3817eb332660dd63d1d4522e63dcc94e79a	O-LIN-ACRN-220721/3318
linux_kernel					
Out-of-bounds Write	07-Jul-21	4.6	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space **CVE ID : CVE-2021-22555**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/net/netfilter/x_tables.c?id=b29c457a6511435960115c0f548c4360d5f4801d	O-LIN-LINU-220721/3319
Improper Neutralization of Input During Web Page Generation ('Cross-site	09-Jul-21	4.3	IBM InfoSphere Information Server 11.7 is vulnerable to 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/6468581, https://exchange.xforce.i	O-LIN-LINU-220721/3320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 200966. **CVE ID : CVE-2021-29712**	bmcloud.com/vulnerabilities/200966	
Improper Verification of Cryptographic Signature	07-Jul-21	6.9	kernel/module.c in the Linux kernel before 5.12.14 mishandles Signature Verification, aka CID-0c18f29aae7c. Without CONFIG_MODULE_SIG, verification that a kernel module is signed, for loading via init_module, does not occur for a module.sig_enforce=1 command-line argument. **CVE ID : CVE-2021-35039**	https://github.com/torvalds/linux/commit/0c18f29aae7ce3daddd26d8ee3505d07cc982df75, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.12.14	O-LIN-LINU-220721/3321
Use After Free	01-Jul-21	6.8	Tesseract OCR 5.0.0-alpha-20201231 has a one_ell_conflict use-after-free during a strpbrk call. **CVE ID : CVE-2021-36081**	https://github.com/tesseract-ocr/tesseract/commit/e6f15621c2ab2ecbfabf656942d8ef66f03b2d55, https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=29698	O-LIN-LINU-220721/3322
Out-of-bounds Write	01-Jul-21	6.8	Grok 7.6.6 through 9.2.0 has a heap-based buffer overflow in grk::FileFormatDecompress::apply_palette_clr (called	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=33	O-LIN-LINU-220721/3323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from grk::FileFormatDecompress::applyColour). **CVE ID : CVE-2021-36089**	544	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-21	7.2	An out-of-bounds memory write flaw was found in the Linux kernel's joystick devices subsystem in versions before 5.9-rc1, in the way the user calls ioctl JSIOCSBTNMAP. This flaw allows a local user to crash the system or possibly escalate their privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2021-3612**	https://lore.kernel.org/linux-input/20210620120030.1513655-1-avlarkin82@gmail.com/	O-LIN-LINU-220721/3324
tizen					
Incorrect Authorization	08-Jul-21	2.1	Improper authorization vulnerability in Tizen factory reset policy prior to Firmware update JUL-2021 Release allows untrusted applications to perform factory reset using dbus signal. **CVE ID : CVE-2021-25433**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	O-LIN-TIZE-220721/3325
Improper Input Validation	08-Jul-21	7.5	Improper input validation vulnerability in Tizen bootloader prior to Firmware update JUL-2021 Release allows arbitrary code execution using param partition in wireless firmware download mode.	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	O-LIN-TIZE-220721/3326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25434		
Improper Input Validation	08-Jul-21	7.5	Improper input validation vulnerability in Tizen bootloader prior to Firmware update JUL-2021 Release allows arbitrary code execution using recovery partition in wireless firmware download mode. **CVE ID : CVE-2021-25435**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	O-LIN-TIZE-220721/3327
Improper Input Validation	08-Jul-21	7.5	Improper input validation vulnerability in Tizen FOTA service prior to Firmware update JUL-2021 Release allows arbitrary code execution via Samsung Accessory Protocol. **CVE ID : CVE-2021-25436**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	O-LIN-TIZE-220721/3328
Incorrect Authorization	08-Jul-21	7.5	Improper access control vulnerability in Tizen FOTA service prior to Firmware update JUL-2021 Release allows attackers to arbitrary code execution by replacing FOTA update file. **CVE ID : CVE-2021-25437**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7	O-LIN-TIZE-220721/3329
Microsoft					
windows					
Incorrect Permission Assignment for Critical Resource	12-Jul-21	4.4	Node.js before 16.4.1, 14.17.2, and 12.22.2 is vulnerable to local privilege escalation attacks under certain conditions on Windows platforms. More specifically, improper configuration of permissions in the installation directory	https://nodejs.org/en/blog/vulnerability/july-2021-security-releases/	O-MIC-WIND-220721/3330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows an attacker to perform two different escalation attacks: PATH and DLL hijacking. **CVE ID : CVE-2021-22921**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jul-21	4.3	IBM InfoSphere Information Server 11.7 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: 200966. **CVE ID : CVE-2021-29712**	https://www.ibm.com/support/pages/node/6468581, https://exchange.xforce.ibmcloud.com/vulnerabilities/200966	O-MIC-WIND-220721/3331
Uncontrolled Search Path Element	02-Jul-21	4.4	OpenVPN before version 2.5.3 on Windows allows local users to load arbitrary dynamic loadable libraries via an OpenSSL configuration file if present, which allows the user to run arbitrary code with the same privilege level as the main OpenVPN process (openvpn.exe). **CVE ID : CVE-2021-3606**	https://community.openvpn.net/openvpn/wiki/SecurityAnnouncements, https://community.openvpn.net/openvpn/wiki/CVE-2021-3606	O-MIC-WIND-220721/3332
windows_10					
Improper Privilege Management	02-Jul-21	9	Windows Print Spooler Remote Code Execution Vulnerability **CVE ID : CVE-2021-34527**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527	O-MIC-WIND-220721/3333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
windows_7					
Improper Privilege Management	02-Jul-21	9	Windows Print Spooler Remote Code Execution Vulnerability **CVE ID : CVE-2021-34527**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527	O-MIC-WIND-220721/3334
windows_8.1					
Improper Privilege Management	02-Jul-21	9	Windows Print Spooler Remote Code Execution Vulnerability **CVE ID : CVE-2021-34527**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527	O-MIC-WIND-220721/3335
windows_rt_8.1					
Improper Privilege Management	02-Jul-21	9	Windows Print Spooler Remote Code Execution Vulnerability **CVE ID : CVE-2021-34527**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527	O-MIC-WIND-220721/3336
windows_server_2008					
Improper Privilege Management	02-Jul-21	9	Windows Print Spooler Remote Code Execution Vulnerability **CVE ID : CVE-2021-34527**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527	O-MIC-WIND-220721/3337
windows_server_2012					
Improper Privilege Management	02-Jul-21	9	Windows Print Spooler Remote Code Execution Vulnerability **CVE ID : CVE-2021-34527**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-220721/3338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2021-34527	
windows_server_2016					
Improper Privilege Management	02-Jul-21	9	Windows Print Spooler Remote Code Execution Vulnerability **CVE ID : CVE-2021-34527**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527	O-MIC-WIND-220721/3339
windows_server_2019					
Improper Privilege Management	02-Jul-21	9	Windows Print Spooler Remote Code Execution Vulnerability **CVE ID : CVE-2021-34527**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527	O-MIC-WIND-220721/3340
Qnap					
qts					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-21	7.5	A command injection vulnerabilities have been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.1.1540 build 20210107. QNAP Systems Inc. QuTS hero versions prior to h4.5.1.1582 build 20210217. **CVE ID : CVE-2021-28802**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-29	O-QNA-QTS-220721/3341
Improper Neutralizatio	01-Jul-21	7.5	A command injection vulnerabilities have been	https://www.qnap.com/	O-QNA-QTS-220721/3342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.1.1540 build 20210107. QNAP Systems Inc. QuTS hero versions prior to h4.5.1.1582 build 20210217. **CVE ID : CVE-2021-28804**	zh-tw/security-advisory/qsa-21-29	
Improper Access Control	08-Jul-21	10	An improper access control vulnerability has been reported to affect certain legacy versions of HBS 3. If exploited, this vulnerability allows attackers to compromise the security of the operating system.QNAP have already fixed this vulnerability in the following versions of HBS 3: QTS 4.3.6: HBS 3 v3.0.210507 and later QTS 4.3.4: HBS 3 v3.0.210506 and later QTS 4.3.3: HBS 3 v3.0.210506 and later **CVE ID : CVE-2021-28809**	https://www.qnap.com/en/security-advisory/qsa-21-19	O-QNA-QTS-220721/3343
quts_hero					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Jul-21	7.5	A command injection vulnerabilities have been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a	https://www.qnap.com/zh-tw/security-advisory/qsa-21-29	O-QNA-QUTS-220721/3344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			compromised application. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.1.1540 build 20210107. QNAP Systems Inc. QuTS hero versions prior to h4.5.1.1582 build 20210217. **CVE ID : CVE-2021-28802**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jul-21	7.5	A command injection vulnerabilities have been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.1.1540 build 20210107. QNAP Systems Inc. QuTS hero versions prior to h4.5.1.1582 build 20210217. **CVE ID : CVE-2021-28804**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-29	O-QNA-QUTS-220721/3345
Qualcomm					
apq8009w_firmware					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3346
Out-of-	13-Jul-21	2.1	Possible buffer over read	https://ww	O-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	220721/3347
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3348
apq8009_firmware					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3349
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-APQ8-220721/3350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3351
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3352
apq8017_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3354
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3355
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3357
apq8037_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3358
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the	https://www.qualcomm.com/compan	O-QUA-APQ8-220721/3359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3360
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3361
apq8053_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	O-QUA-APQ8-220721/3362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3363
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3364
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	O-QUA-APQ8-220721/3365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3366
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3367
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3369
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3370
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3371
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	O-QUA-APQ8-220721/3372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3373
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3375
apq8064au_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3376
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3378
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3379
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3381
apq8096au_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3382
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-APQ8-220721/3383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3384
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3385
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-APQ8-220721/3386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-APQ8-220721/3387
aqt1000_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3388
Double Free	13-Jul-21	7.2	Memory corruption in key	https://ww	O-QUA-AQT1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	220721/3389
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3390
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3391
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause	https://www.qualcomm.	O-QUA-AQT1-220721/3392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3393
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3394
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3395
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bull	O-QUA-AQT1-220721/3396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3397
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3398
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-AQT1-220721/3399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3400
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3401
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-AQT1-220721/3402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3403
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3405
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3406
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AQT1-220721/3407
ar6003_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR60-220721/3408
ar7420_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR74-220721/3409
ar8031_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3411
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3412
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3414
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3415
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3417
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3418
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3420
ar8035_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3421
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-AR80-220721/3422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3423
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3424
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-AR80-220721/3425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3426
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3427
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-AR80-220721/3428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3429
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3431
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR80-220721/3432
ar9380_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR93-220721/3433
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while	https://www.qualcomm.	O-QUA-AR93-220721/3434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR93-220721/3435
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR93-220721/3436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR93-220721/3437
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR93-220721/3438
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-AR93-220721/3439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-AR93-220721/3440
csr6030_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSR6-220721/3441
csr8811_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSR8-220721/3442
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSR8-220721/3443
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSR8-220721/3444
Out-of-	13-Jul-21	5	Possible out of bound read	https://ww	O-QUA-CSR8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	220721/3445
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSR8-220721/3446
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSR8-220721/3447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSR8-220721/3448
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSR8-220721/3449
csra6620_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3451
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3452
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3454
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3455
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-CSRA-220721/3456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3457
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3458
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of	https://www.qualcomm.	O-QUA-CSRA-220721/3459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	com/company/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3460
csra6640_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3462
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3463
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3465
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3466
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3468
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3469
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRA-220721/3471
csrb31024_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRB-220721/3472
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-CSRB-220721/3473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRB-220721/3474
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRB-220721/3475
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRB-220721/3476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRB-220721/3477
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRB-220721/3478
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-CSRB-220721/3479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRB-220721/3480
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRB-220721/3481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRB-220721/3482
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-CSRB-220721/3483
fsm10055_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3485
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3486
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1890		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3488
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3489
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1940		
fsm10056_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3491
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3492
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3494
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3495
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-FSM1-220721/3496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq4018_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3497
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3498
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3500
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3501
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3503
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3504
ipq4019_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-IPQ4-220721/3505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1887	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3506
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3507
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3509
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3510
ipq4028_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3512
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3513
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3515
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3516
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	O-QUA-IPQ4-220721/3517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3518
ipq4029_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3519
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3521
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3522
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to	https://www.qualcomm.com/compan	O-QUA-IPQ4-220721/3523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3524
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ4-220721/3526
ipq5010_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3527
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3529
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3530
Out-of-	13-Jul-21	5	Possible buffer over read	https://ww	O-QUA-IPQ5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	220721/3531
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3532
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3533
ipq5018_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3534
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3535
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3537
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3538
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	O-QUA-IPQ5-220721/3539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3540
ipq5028_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3542
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3543
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3545
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ5-220721/3546
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ5-220721/3547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	etins/july-2021-bulletin	
ipq6000_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3548
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3549
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	O-QUA-IPQ6-220721/3550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3551
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3553
ipq6005_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3554
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-IPQ6-220721/3555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3556
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3558
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3559
ipq6010_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3561
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3562
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3564
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3565
Improper	13-Jul-21	10	Possible buffer overflow due	https://ww	O-QUA-IPQ6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	220721/3566
ipq6018_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3567
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3569
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3570
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ6-220721/3571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3572
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3573
ipq6028_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-IPQ6-220721/3574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3575
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3577
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3578
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-IPQ6-220721/3579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ6-220721/3580
ipq8064_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3581
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3583
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3584
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-IPQ8-220721/3585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3586
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3588
ipq8065_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3589
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3590
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	O-QUA-IPQ8-220721/3591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3592
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3594
ipq8068_firmware					
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3595
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3597
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3598
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1965		
ipq8069_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3600
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3601
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
ipq8070a_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3603
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3604
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	O-QUA-IPQ8-220721/3605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3606
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3608
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3609
ipq8070_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3611
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3612
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ8-220721/3613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3614
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3616
ipq8071a_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3617
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3619
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3620
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing	https://www.qualcomm.com/compan	O-QUA-IPQ8-220721/3621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3622
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3623
ipq8071_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while	https://www.qualcomm.	O-QUA-IPQ8-220721/3624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3625
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3627
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3628
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ8-220721/3629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	etins/july-2021-bulletin	
ipq8072a_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3630
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1943		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3632
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3633
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-IPQ8-220721/3634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3635
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3636
ipq8072_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ8-220721/3637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3638
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3640
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3641
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
ipq8074a_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3643
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3644
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	O-QUA-IPQ8-220721/3645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3646
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3648
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3649
ipq8074_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3651
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3652
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3654
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3655
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	O-QUA-IPQ8-220721/3656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
ipq8076a_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3657
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3659
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3660
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-220721/3661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3662
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3663
ipq8076_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	O-QUA-IPQ8-220721/3664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3665
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3667
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3668
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-IPQ8-220721/3669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3670
ipq8078a_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3671
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	O-QUA-IPQ8-220721/3672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3673
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3675
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3676
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
ipq8078_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3678
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3679
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-IPQ8-220721/3680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3681
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3683
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3684
ipq8173_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3686
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3687
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-IPQ8-220721/3688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3689
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3691
ipq8174_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3692
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3694
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3695
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-220721/3696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3697
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-IPQ8-220721/3698
mdm8215m_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when	https://www.qualcomm.com/compan	O-QUA-MDM8-220721/3699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	y/product-security/bulletins/july-2021-bulletin	
mdm8215_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM8-220721/3700
mdm8615m_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM8-220721/3701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
mdm9150_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3702
mdm9205_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3704
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3705
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mdm9206_firmware					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3707
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3708
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3709
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
mdm9215_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3711
mdm9230_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
mdm9250_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3713
mdm9310_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3714
mdm9330_firmware					
Reachable	13-Jul-21	5	Denial of service in SAP case	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	MDM9-220721/3715
mdm9607_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3716
mdm9615m_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-MDM9-220721/3717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	2021-bulletin	
mdm9615_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3718
mdm9626_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
mdm9628_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3720
mdm9630_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mdm9640_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3722
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3723
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1889		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3725
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3726
mdm9650_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3728
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3729
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3731
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3732
mdm9655_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	O-QUA-MDM9-220721/3733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3734
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MDM9-220721/3735
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	O-QUA-MDM9-220721/3736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
msm8909w_firmware					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3737
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3738
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
msm8917_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3740
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3741
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-MSM8-220721/3742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3743
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3744
msm8920_firmware					
Out-of-bounds	13-Jul-21	7.2	Incorrect handling of pointers in trusted	https://www.qualcomm.	O-QUA-MSM8-220721/3745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	com/company/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3746
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3747
Improper Restriction	13-Jul-21	7.2	Improper length check of public exponent in RSA	https://www.qualcomm.	O-QUA-MSM8-220721/3748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	com/company/product-security/bulletins/july-2021-bulletin	
msm8937_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3749
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3751
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3752
msm8940_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3754
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3755
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
msm8953_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3757
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3758
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1889		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3760
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3761
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3762
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	O-QUA-MSM8-220721/3763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3764
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3766
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3767
msm8996au_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3769
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3770
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1890**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3772
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-MSM8-220721/3773
pm8937_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-PM89-220721/3774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-PM89-220721/3775
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-PM89-220721/3776
Improper Restriction of Operations within the Bounds of a	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-PM89-220721/3777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	2021-bulletin	
pmp8074_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-PMP8-220721/3778
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-PMP8-220721/3779
Out-of-	13-Jul-21	5	Possible out of bound read	https://ww	O-QUA-PMP8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	220721/3780
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-PMP8-220721/3781
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-PMP8-220721/3782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-PMP8-220721/3783
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-PMP8-220721/3784
qca1062_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA1-220721/3785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA1-220721/3786
qca1064_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA1-220721/3787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA1-220721/3788
qca2062_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA2-220721/3789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA2-220721/3790
qca2064_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA2-220721/3791
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while	https://www.qualcomm.com/company/product-	O-QUA-QCA2-220721/3792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	security/bulletins/july-2021-bulletin	
qca2065_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA2-220721/3793
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA2-220721/3794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
qca2066_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA2-220721/3795
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA2-220721/3796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
qca4004_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3797
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3798
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA4-220721/3799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3800
qca4020_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3801
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in	https://www.qualcomm.com/company/product-	O-QUA-QCA4-220721/3802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3803
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3804
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA4-220721/3805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3806
qca4024_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3807
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	O-QUA-QCA4-220721/3808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3809
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3811
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3812
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA4-220721/3813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
qca6164_firmware					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3814
qca6174a_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3815
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3817
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3818
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3819
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer	https://www.qualcomm.com/company/product-	O-QUA-QCA6-220721/3820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3821
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3822
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA6-220721/3823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3824
qca6174_firmware					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3825
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when	https://www.qualcomm.com/compan	O-QUA-QCA6-220721/3826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	y/product-security/bulletins/july-2021-bulletin	
qca6175a_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3827
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3829
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3830
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3831
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	O-QUA-QCA6-220721/3832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3833
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3835
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3836
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCA6-220721/3837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	security/bulletins/july-2021-bulletin	
qca6234_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3838
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3839
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCA6-220721/3840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3841
qca6310_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3842
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3844
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3845
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-220721/3846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3847
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6320_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3849
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3850
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3851
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in	https://www.qualcomm.com/compan	O-QUA-QCA6-220721/3852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	y/product-security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3853
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3854
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-220721/3855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3856
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3858
qca6335_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3859
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3860
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	O-QUA-QCA6-220721/3861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3862
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3864
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3865
qca6390_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-220721/3866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3867
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3868
Improper Restriction of Operations within the Bounds of a	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-220721/3869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3870
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3871
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3873
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3874
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-220721/3875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3876
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3878
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3879
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6391_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3881
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3882
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1889		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3884
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3885
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3886
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCA6-220721/3887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	security/bulletins/july-2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3888
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3889
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	O-QUA-QCA6-220721/3890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3891
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3893
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3894
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-220721/3895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3896
qca6420_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3897
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA6-220721/3898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3899
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3900
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3902
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3903
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3904
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3905
Buffer Copy without	13-Jul-21	7.2	Possible buffer overflow due to improper validation of	https://www.qualcomm.	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	com/company/product-security/bulletins/july-2021-bulletin	220721/3906
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3907
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3908
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to	https://www.qualcomm.	O-QUA-QCA6-220721/3909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3910
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3912
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3913
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-220721/3914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3915
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3916
qca6421_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA6-220721/3917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3918
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3919
Improper Restriction of Operations within the Bounds of a Memory	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA6-220721/3920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3921
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3922
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-220721/3923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3924
qca6426_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3926
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3927
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3929
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3930
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3932
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3933
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3935
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3937
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3938
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3939
qca6428_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem	https://www.qualcomm.	O-QUA-QCA6-220721/3940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3941
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3942
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	O-QUA-QCA6-220721/3943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3944
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1964**		
qca6430_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3946
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3947
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3949
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3950
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3951
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QCA6-220721/3952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3953
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3954
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3955
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCA6-220721/3956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	security/bulletins/july-2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3957
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3958
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	O-QUA-QCA6-220721/3959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3960
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3962
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3963
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-220721/3964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3965
qca6431_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3966
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA6-220721/3967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3968
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3969
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3971
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3972
Reachable	13-Jul-21	5	Denial of service in SAP case	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	220721/3973
qca6436_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3974
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3976
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3977
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3979
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3980
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3982
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3983
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-220721/3984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3985
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3987
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3988
qca6438_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3989
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3991
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3992
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to	https://www.qualcomm.com/compan	O-QUA-QCA6-220721/3993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3994
qca6564au_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3996
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3997
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/3999
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4000
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4002
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4003
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4005
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4006
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	O-QUA-QCA6-220721/4007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4008
qca6564a_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4009
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function	https://www.qualcomm.	O-QUA-QCA6-220721/4010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	com/company/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4011
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4012
Buffer Copy without Checking	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto,	https://www.qualcomm.com/compan	O-QUA-QCA6-220721/4013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4014
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4015
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-220721/4016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4017
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4018
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-220721/4019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4020
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4022
qca6564_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4023
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4025
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4026
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1931		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4028
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4029
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4031
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4032
qca6574au_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4034
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4035
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4037
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4038
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1938		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4040
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4041
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4043
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4044
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-220721/4045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4046
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4047
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCA6-220721/4048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	security/bulletins/july-2021-bulletin	
qca6574a_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4049
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4050
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCA6-220721/4051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4052
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4053
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4055
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4056
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4058
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4059
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	O-QUA-QCA6-220721/4060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4061
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4063
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4064
qca6574_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4066
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4067
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4069
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4070
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4071
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of	https://www.qualcomm.	O-QUA-QCA6-220721/4072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4073
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4074
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR	https://www.qualcomm.	O-QUA-QCA6-220721/4075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4076
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4078
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4079
qca6584au_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA6-220721/4080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4081
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4082
Improper Restriction of Operations within the Bounds of a Memory	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA6-220721/4083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4084
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4085
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4087
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4088
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4090
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4091
Improper	13-Jul-21	5	Possible buffer over read	https://ww	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	220721/4092
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4093
qca6584_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
qca6595au_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4095
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4096
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4098
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4099
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4100
Reachable	13-Jul-21	5	Possible assertion due to improper verification while	https://www.qualcomm.	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	com/company/product-security/bulletins/july-2021-bulletin	220721/4101
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4102
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4104
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4105
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4107
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4108
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE	https://www.qualcomm.com/compan	O-QUA-QCA6-220721/4109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4110
qca6595_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4111
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-220721/4112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4113
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4114
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-220721/4115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4116
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4117
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-220721/4118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4119
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4121
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4122
qca6694au_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4124
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4125
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1890**		
qca6694_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4127
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4128
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4130
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4131
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
qca6696_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4133
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4134
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-220721/4135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4136
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4137
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1931		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4139
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4140
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4142
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4143
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in	https://www.qualcomm.com/company/product-	O-QUA-QCA6-220721/4144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4145
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4147
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA6-220721/4148
qca7500_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA7-220721/4149
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA7-220721/4150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA7-220721/4151
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA7-220721/4152
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	O-QUA-QCA7-220721/4153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA7-220721/4154
qca7520_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA7-220721/4155
qca7550_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA7-220721/4156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1887**	2021-bulletin	
qca8072_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4157
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4158
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA8-220721/4159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4160
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4162
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4163
qca8075_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4165
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4166
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA8-220721/4167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4168
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4170
qca8081_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4171
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4173
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4174
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in	https://www.qualcomm.com/company/product-	O-QUA-QCA8-220721/4175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4176
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4177
qca8337_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	O-QUA-QCA8-220721/4178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4179
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4180
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	O-QUA-QCA8-220721/4181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4182
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4183
Use After	13-Jul-21	7.2	Use after free can occur due	https://ww	O-QUA-QCA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	220721/4184
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4185
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4187
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA8-220721/4188
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA8-220721/4189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	bulletin	
qca9367_firmware					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4190
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4191
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4192
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in	https://www.qualcomm.com/company/product-	O-QUA-QCA9-220721/4193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	security/bulletins/july-2021-bulletin	
qca9377_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4194
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4196
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4197
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4198
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1898**		
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4200
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4201
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4203
qca9379_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4204
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA9-220721/4205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4206
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4207
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA9-220721/4208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1899	bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4209
qca9531_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4210
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1943		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4212
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4213
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
qca9558_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4215
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4216
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4218
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4219
qca9561_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1887		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4221
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4222
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4224
qca9563_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4225
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4227
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4228
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
qca9880_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4230
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4231
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4233
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4234
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
qca9882_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4236
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4237
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
qca9886_firmware					
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4239
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4240
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4242
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4243
qca9887_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1887		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4245
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4246
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4248
qca9888_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4249
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4251
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4252
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA9-220721/4253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4254
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4256
qca9889_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4257
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4258
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT	https://www.qualcomm.com/compan	O-QUA-QCA9-220721/4259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4260
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4262
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4263
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
qca9896_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4265
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4266
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4268
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4269
qca9898_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4271
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4272
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4274
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4275
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	O-QUA-QCA9-220721/4276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4277
qca9980_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4278
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4280
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4281
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to	https://www.qualcomm.com/compan	O-QUA-QCA9-220721/4282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4283
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4285
qca9982_firmware					
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4286
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4288
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4289
qca9984_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA9-220721/4290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1887**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4291
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4292
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCA9-220721/4293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4294
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4296
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4297
qca9985_firmware					
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1943		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4299
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4300
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4302
qca9990_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4303
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1938		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4305
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4306
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4308
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4309
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE	https://www.qualcomm.com/compan	O-QUA-QCA9-220721/4310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	y/product-security/bulletins/july-2021-bulletin	
qca9992_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4311
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4312
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA9-220721/4313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4314
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4316
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4317
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1965		
qca9994_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4319
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4320
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1943		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4322
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4323
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA9-220721/4324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4325
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCA9-220721/4326
qcm2290_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCM2-220721/4327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	etins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM2-220721/4328
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM2-220721/4329
Improper Restriction of Operations within the	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCM2-220721/4330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM2-220721/4331
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM2-220721/4332
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	O-QUA-QCM2-220721/4333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM2-220721/4334
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM2-220721/4335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM2-220721/4336
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM2-220721/4337
qcm4290_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4339
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4340
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4342
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4343
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4345
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4346
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4348
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM4-220721/4349
qcm6125_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCM6-220721/4350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	etins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM6-220721/4351
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM6-220721/4352
Improper Restriction of Operations within the	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCM6-220721/4353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM6-220721/4354
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM6-220721/4355
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM6-220721/4356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM6-220721/4357
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM6-220721/4358
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM6-220721/4359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM6-220721/4360
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM6-220721/4361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCM6-220721/4362
qcn5021_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4363
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4365
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4366
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing	https://www.qualcomm.com/compan	O-QUA-QCN5-220721/4367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4368
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4369
qcn5022_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while	https://www.qualcomm.	O-QUA-QCN5-220721/4370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4371
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4373
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4374
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-220721/4375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4376
qcn5024_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4377
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4379
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4380
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-220721/4381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4382
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4384
qcn5052_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4385
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4387
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4388
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing	https://www.qualcomm.com/compan	O-QUA-QCN5-220721/4389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4390
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4391
qcn5054_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem	https://www.qualcomm.	O-QUA-QCN5-220721/4392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4393
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4394
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	O-QUA-QCN5-220721/4395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4396
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4398
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4399
qcn5064_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4401
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4402
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-220721/4403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4404
qcn5121_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4406
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4407
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCN5-220721/4408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4409
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4410
qcn5122_firmware					
Reachable	13-Jul-21	5	Possible assertion due to	https://ww	O-QUA-QCN5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	220721/4411
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4412
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4414
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4415
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in	https://www.qualcomm.com/company/product-	O-QUA-QCN5-220721/4416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4417
qcn5124_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4418
Out-of-	13-Jul-21	5	Possible buffer out of bound	https://ww	O-QUA-QCN5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	220721/4419
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4420
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4422
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4423
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCN5-220721/4424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	2021-bulletin	
qcn5152_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4425
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4426
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	O-QUA-QCN5-220721/4427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4428
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4430
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4431
qcn5154_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4433
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4434
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-220721/4435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4436
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4438
qcn5164_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4439
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4441
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4442
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing	https://www.qualcomm.com/compan	O-QUA-QCN5-220721/4443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4444
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4445
qcn5500_firmware					
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to	https://www.qualcomm.	O-QUA-QCN5-220721/4446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4447
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4449
qcn5501_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4450
qcn5502_firmware					
Reachable Assertion	13-Jul-21	5	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1887**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4451
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN5-220721/4452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4453
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4454
Improper Input	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	O-QUA-QCN5-220721/4455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	com/company/product-security/bulletins/july-2021-bulletin	
qcn5550_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4456
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4458
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4459
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	O-QUA-QCN5-220721/4460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN5-220721/4461
qcn6023_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4463
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4464
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4466
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4467
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN6-220721/4468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	etins/july-2021-bulletin	
qcn6024_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4469
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4470
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	O-QUA-QCN6-220721/4471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4472
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4474
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4475
qcn6122_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4477
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4478
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while	https://www.qualcomm.com/company/product-	O-QUA-QCN6-220721/4479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4480
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN6-220721/4482
qcn7605_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN7-220721/4483
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN7-220721/4484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
qcn7606_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN7-220721/4485
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN7-220721/4486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
qcn9000_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4487
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4488
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	O-QUA-QCN9-220721/4489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4490
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4492
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4493
qcn9012_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4495
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4496
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN9-220721/4497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4498
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4500
qcn9022_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4501
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4503
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4504
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing	https://www.qualcomm.com/compan	O-QUA-QCN9-220721/4505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4506
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4507
qcn9024_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while	https://www.qualcomm.	O-QUA-QCN9-220721/4508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4509
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4511
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4512
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCN9-220721/4513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4514
qcn9070_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4515
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to	https://www.qualcomm.	O-QUA-QCN9-220721/4516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4517
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4519
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4520
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QCN9-220721/4521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	bulletin	
qcn9072_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4522
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4523
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCN9-220721/4524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4525
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1954**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4527
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4528
qcn9074_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4530
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4531
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCN9-220721/4532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4533
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1964		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4535
qcn9100_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4536
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4538
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4539
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing	https://www.qualcomm.com/compan	O-QUA-QCN9-220721/4540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4541
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCN9-220721/4542
qcs2290_firmware					
Out-of-bounds	13-Jul-21	7.2	Incorrect handling of pointers in trusted	https://www.qualcomm.	O-QUA-QCS2-220721/4543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	com/company/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS2-220721/4544
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS2-220721/4545
Improper Restriction	13-Jul-21	7.2	Improper length check of public exponent in RSA	https://www.qualcomm.	O-QUA-QCS2-220721/4546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	com/company/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS2-220721/4547
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS2-220721/4548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS2-220721/4549
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS2-220721/4550
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS2-220721/4551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS2-220721/4552
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS2-220721/4553
qcs405_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS4-220721/4554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	etins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4555
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4556
Improper Restriction of Operations within the	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS4-220721/4557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4558
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4559
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in	https://www.qualcomm.com/compan	O-QUA-QCS4-220721/4560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4561
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4563
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4564
qcs410_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4566
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4567
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4569
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4570
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4572
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4573
qcs4290_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	O-QUA-QCS4-220721/4574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4575
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4576
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	O-QUA-QCS4-220721/4577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4578
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4579
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4581
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4582
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when	https://www.qualcomm.com/compan	O-QUA-QCS4-220721/4583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4584
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS4-220721/4585
qcs603_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-220721/4586
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-220721/4587
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-220721/4588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-220721/4589
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-220721/4590
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-220721/4591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1938		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-220721/4592
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-220721/4593
qcs605_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	O-QUA-QCS6-230721/4594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4595
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4596
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	O-QUA-QCS6-230721/4597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4598
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4599
Reachable	13-Jul-21	5	Improper handling of	https://ww	O-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4600
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4601
qcs610_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS6-230721/4602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	etins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4603
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4604
Improper Restriction of Operations within the	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS6-230721/4605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4606
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4607
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in	https://www.qualcomm.com/compan	O-QUA-QCS6-230721/4608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4609
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4611
qcs6125_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4612
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4614
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4615
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4616
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot	https://www.qualcomm.com/company/product-	O-QUA-QCS6-230721/4617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4618
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4619
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCS6-230721/4620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4621
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4623
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QCS6-230721/4624
qet4101_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QET4-230721/4625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
qsm8250_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QSM8-230721/4626
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QSM8-230721/4627
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QSM8-230721/4628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QSM8-230721/4629
qsm8350_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QSM8-230721/4630
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the	https://www.qualcomm.com/compan	O-QUA-QSM8-230721/4631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QSM8-230721/4632
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QSM8-230721/4633
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QSM8-230721/4634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QSM8-230721/4635
qsw8573_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QSW8-230721/4636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
qualcomm215_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QUAL-230721/4637
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QUAL-230721/4638
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in	https://www.qualcomm.com/compan	O-QUA-QUAL-230721/4639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	y/product-security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QUAL-230721/4640
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QUAL-230721/4641
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-QUAL-230721/4642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QUAL-230721/4643
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QUAL-230721/4644
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-QUAL-230721/4645
sa415m_firmware					
Out-of-	13-Jul-21	7.2	Incorrect handling of	https://ww	O-QUA-SA41-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4646
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA41-230721/4647
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA41-230721/4648
Improper	13-Jul-21	7.2	Improper length check of	https://ww	O-QUA-SA41-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4649
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA41-230721/4650
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA41-230721/4651
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA41-230721/4652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA41-230721/4653
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA41-230721/4654
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SA41-230721/4655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA41-230721/4656
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA41-230721/4657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA41-230721/4658
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA41-230721/4659
sa515m_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4661
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4662
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4664
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4665
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1940		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4667
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4668
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4670
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA51-230721/4671
Improper	13-Jul-21	5	Possible out of bound read	https://ww	O-QUA-SA51-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4672
sa6145p_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4673
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4674
Buffer Copy	13-Jul-21	7.2	Possible buffer overflow due	https://ww	O-QUA-SA61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4675
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4676
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4677
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA61-230721/4678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4679
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4680
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA61-230721/4681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4682
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4684
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4685
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4687
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4688
sa6150p_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4690
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4691
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4693
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4694
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1938		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4696
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4697
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4699
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4700
Improper	13-Jul-21	5	Possible buffer over read	https://ww	O-QUA-SA61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4701
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4702
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4703
sa6155p_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	O-QUA-SA61-230721/4704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4705
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4706
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	O-QUA-SA61-230721/4707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4708
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4709
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4711
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4712
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA61-230721/4713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4714
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4716
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4717
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4719
sa6155_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4720
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4722
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4723
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4724
Buffer Copy without	13-Jul-21	7.2	Possible buffer overflow due to improper validation of	https://www.qualcomm.	O-QUA-SA61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	com/company/product-security/bulletins/july-2021-bulletin	230721/4725
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4726
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4727
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to	https://www.qualcomm.	O-QUA-SA61-230721/4728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4729
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4731
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4732
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA61-230721/4733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA61-230721/4734
sa8145p_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4735
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in	https://www.qualcomm.com/company/product-	O-QUA-SA81-230721/4736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4737
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4738
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-230721/4739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4740
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4741
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SA81-230721/4742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4743
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4745
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4746
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4748
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4749
sa8150p_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4751
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4752
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1890		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4754
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4755
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4756
Out-of-	13-Jul-21	5	Possible buffer out of bound	https://ww	O-QUA-SA81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4757
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4758
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4760
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4761
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in	https://www.qualcomm.com/company/product-	O-QUA-SA81-230721/4762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4763
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4764
sa8155p_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA81-230721/4765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4766
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4767
Improper Restriction of Operations within the Bounds of a	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SA81-230721/4768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4769
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4770
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4772
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4773
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4775
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4776
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of	https://www.qualcomm.	O-QUA-SA81-230721/4777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	com/company/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4778
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4780
sa8155_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4781
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4783
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4784
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4785
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-230721/4786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4787
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4788
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-230721/4789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4790
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4792
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4793
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4795
sa8195p_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4796
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SA81-230721/4797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4798
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4799
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1907		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4801
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4802
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1940		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4804
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4805
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4807
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4808
Improper	13-Jul-21	5	Possible buffer over read	https://ww	O-QUA-SA81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4809
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4810
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SA81-230721/4811
sc8180x\\+sdx55_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	O-QUA-SC81-230721/4812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SC81-230721/4813
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SC81-230721/4814
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	O-QUA-SC81-230721/4815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SC81-230721/4816
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SC81-230721/4817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
sc8180x_firmware					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SC81-230721/4818
sc8280xp_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SC82-230721/4819
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SC82-230721/4820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
sd205_firmware					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD20-230721/4821
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD20-230721/4822
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD20-230721/4823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1899		
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD20-230721/4824
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD20-230721/4825
sd210_firmware					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD21-230721/4826
Out-of-	13-Jul-21	2.1	Possible buffer over-read	https://ww	O-QUA-SD21-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4827
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD21-230721/4828
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD21-230721/4829
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD21-230721/4830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
sd429_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD42-230721/4831
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD42-230721/4832
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD42-230721/4833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD42-230721/4834
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD42-230721/4835
sd439_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD43-230721/4836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	etins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD43-230721/4837
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD43-230721/4838
Improper Restriction of Operations within the	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD43-230721/4839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD43-230721/4840
sd450_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD45-230721/4841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD45-230721/4842
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD45-230721/4843
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD45-230721/4844
Reachable	13-Jul-21	5	Denial of service in SAP case	https://ww	O-QUA-SD45-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4845
sd460_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD46-230721/4846
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD46-230721/4847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD46-230721/4848
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD46-230721/4849
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD46-230721/4850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD46-230721/4851
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD46-230721/4852
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD46-230721/4853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD46-230721/4854
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD46-230721/4855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD46-230721/4856
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD46-230721/4857
sd480_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD48-230721/4858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD48-230721/4859
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD48-230721/4860
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD48-230721/4861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1890		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD48-230721/4862
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD48-230721/4863
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD48-230721/4864
Out-of-	13-Jul-21	5	Possible buffer out of bound	https://ww	O-QUA-SD48-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4865
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD48-230721/4866
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD48-230721/4867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD48-230721/4868
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD48-230721/4869
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD48-230721/4870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	security/bulletins/july-2021-bulletin	
sd632_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD63-230721/4871
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD63-230721/4872
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD63-230721/4873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD63-230721/4874
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD63-230721/4875
sd660_firmware					
Out-of-	13-Jul-21	7.2	Incorrect handling of	https://ww	O-QUA-SD66-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4876
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4877
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4878
Improper	13-Jul-21	7.2	Improper length check of	https://ww	O-QUA-SD66-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4879
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4880
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4881
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD66-230721/4882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4883
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4884
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD66-230721/4885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4886
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4888
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4889
sd662_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4891
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4892
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4894
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4895
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD66-230721/4896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4897
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4899
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4900
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1970		
sd665_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4902
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4903
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4905
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4906
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4907
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	O-QUA-SD66-230721/4908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4909
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4910
Out-of-	13-Jul-21	5	Possible out of bound read	https://ww	O-QUA-SD66-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4911
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4912
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4914
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD66-230721/4915
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD66-230721/4916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	security/bulletins/july-2021-bulletin	
sd670_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4917
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4918
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD67-230721/4919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4920
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4921
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4923
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4924
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD67-230721/4925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4926
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4928
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4929
sd675_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4931
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4932
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1890**		
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4934
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4935
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4936
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1901		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4938
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4939
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1940		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4941
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4942
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4944
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4945
Improper	13-Jul-21	5	Possible buffer over read	https://ww	O-QUA-SD67-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/4946
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4947
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4948
sd678_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	O-QUA-SD67-230721/4949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4950
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4951
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	O-QUA-SD67-230721/4952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4953
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4954
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4956
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4957
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4958
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of	https://www.qualcomm.	O-QUA-SD67-230721/4959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4960
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4961
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR	https://www.qualcomm.	O-QUA-SD67-230721/4962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4963
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4965
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4966
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD67-230721/4967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**		
sd690_5g_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD69-230721/4968
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD69-230721/4969
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD69-230721/4970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD69-230721/4971
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD69-230721/4972
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD69-230721/4973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD69-230721/4974
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD69-230721/4975
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD69-230721/4976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD69-230721/4977
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD69-230721/4978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD69-230721/4979
sd710_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD71-230721/4980
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD71-230721/4981
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while	https://www.qualcomm.	O-QUA-SD71-230721/4982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD71-230721/4983
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD71-230721/4984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD71-230721/4985
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD71-230721/4986
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	O-QUA-SD71-230721/4987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD71-230721/4988
sd712_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD71-230721/4989
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function	https://www.qualcomm.	O-QUA-SD71-230721/4990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	com/company/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD71-230721/4991
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD71-230721/4992
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	O-QUA-SD71-230721/4993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD71-230721/4994
sd720g_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD72-230721/4995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/4996
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/4997
Improper Restriction of Operations within the Bounds of a Memory	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD72-230721/4998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/4999
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/5000
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/5001
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD72-230721/5002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/5003
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/5004
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD72-230721/5005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/5006
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/5007
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD72-230721/5008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/5009
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/5010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/5011
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/5012
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD72-230721/5013
sd730_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5014
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5015
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5017
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5018
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5019
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD73-230721/5020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1899**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5021
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5022
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5024
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5025
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5027
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5028
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5030
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD73-230721/5031
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD73-230721/5032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	2021-bulletin	
sd750g_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD75-230721/5033
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD75-230721/5034
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD75-230721/5035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD75-230721/5036
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD75-230721/5037
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD75-230721/5038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD75-230721/5039
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD75-230721/5040
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to	https://www.qualcomm.com/compan	O-QUA-SD75-230721/5041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD75-230721/5042
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD75-230721/5043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD75-230721/5044
sd765g_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5045
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5047
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5048
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5050
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5051
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5053
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5054
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD76-230721/5055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5056
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5058
sd765_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5059
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5061
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5062
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5063
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD76-230721/5064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5065
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5066
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	O-QUA-SD76-230721/5067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5068
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5070
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5071
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD76-230721/5072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	etins/july-2021-bulletin	
sd768g_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5073
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5074
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD76-230721/5075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5076
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5077
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5079
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5080
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD76-230721/5081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5082
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5084
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5085
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD76-230721/5086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1970		
sd778g_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5087
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5088
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5090
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5091
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5092
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	O-QUA-SD77-230721/5093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5094
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5096
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5097
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD77-230721/5098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5099
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD77-230721/5100
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD77-230721/5101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	security/bulletins/july-2021-bulletin	
sd780g_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5102
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5103
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD78-230721/5104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5105
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5106
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5108
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5109
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD78-230721/5110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5111
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5113
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5114
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD78-230721/5116
sd7c_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD7C-230721/5117
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD7C-230721/5118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD7C-230721/5119
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD7C-230721/5120
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD7C-230721/5121
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	O-QUA-SD7C-230721/5122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD7C-230721/5123
sd820_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD82-230721/5124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD82-230721/5125
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD82-230721/5126
Improper Restriction of Operations within the Bounds of a Memory	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD82-230721/5127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	bulletin	
sd821_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD82-230721/5128
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD82-230721/5129
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD82-230721/5130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD82-230721/5131
sd835_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD83-230721/5132
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in	https://www.qualcomm.com/company/product-	O-QUA-SD83-230721/5133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD83-230721/5134
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD83-230721/5135
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD83-230721/5136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD83-230721/5137
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD83-230721/5138
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD83-230721/5139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD83-230721/5140
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD83-230721/5141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD83-230721/5142
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD83-230721/5143
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD83-230721/5144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1970		
sd845_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD84-230721/5145
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD84-230721/5146
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD84-230721/5147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD84-230721/5148
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD84-230721/5149
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD84-230721/5150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD84-230721/5151
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD84-230721/5152
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in	https://www.qualcomm.com/compan	O-QUA-SD84-230721/5153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	y/product-security/bulletins/july-2021-bulletin	
sd850_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5154
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5155
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in	https://www.qualcomm.com/compan	O-QUA-SD85-230721/5156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	y/product-security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5157
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5158
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5160
sd855_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5162
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5163
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5165
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5166
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5167
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5168
Buffer Copy without	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA	https://www.qualcomm.	O-QUA-SD85-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	com/company/product-security/bulletins/july-2021-bulletin	230721/5169
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5170
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5171
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD85-230721/5172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5173
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5174
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while	https://www.qualcomm.com/company/product-	O-QUA-SD85-230721/5175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5176
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5178
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5179
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD85-230721/5180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1970		
sd865_5g_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5181
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5182
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5184
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5185
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5186
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the	https://www.qualcomm.com/compan	O-QUA-SD86-230721/5187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5188
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1945		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5190
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5191
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD86-230721/5192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5193
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD86-230721/5194
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD86-230721/5195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	security/bulletins/july-2021-bulletin	
sd870_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5196
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5197
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD87-230721/5198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	security/bulletins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5199
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5200
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5202
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5203
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD87-230721/5204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5205
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5207
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5208
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD87-230721/5210
sd888_5g_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5211
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5213
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5214
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5215
Buffer Copy without	13-Jul-21	7.2	Possible buffer overflow due to improper validation of	https://www.qualcomm.	O-QUA-SD88-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	com/company/product-security/bulletins/july-2021-bulletin	230721/5216
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5217
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1943		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5219
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5220
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SD88-230721/5221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5222
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5223
Improper	13-Jul-21	10	Possible buffer overflow due	https://ww	O-QUA-SD88-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/5224
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5225
sd888_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5226
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5228
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5229
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD88-230721/5230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5231
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5233
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5234
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD88-230721/5235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sda429w_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDA4-230721/5236
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDA4-230721/5237
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDA4-230721/5238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1889		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDA4-230721/5239
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDA4-230721/5240
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDA4-230721/5241
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDA4-230721/5242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDA4-230721/5243
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDA4-230721/5244
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDA4-230721/5245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdm429w_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM4-230721/5246
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM4-230721/5247
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM4-230721/5248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1889		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM4-230721/5249
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM4-230721/5250
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM4-230721/5251
sdm630_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM6-230721/5252
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM6-230721/5253
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM6-230721/5254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM6-230721/5255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM6-230721/5256
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM6-230721/5257
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDM6-230721/5258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	etins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM6-230721/5259
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM6-230721/5260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM6-230721/5261
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM6-230721/5262
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SDM6-230721/5263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM6-230721/5264
sdm830_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM8-230721/5265
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SDM8-230721/5266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM8-230721/5267
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDM8-230721/5268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
sdw2500_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDW2-230721/5269
sdx20m_firmware					
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX2-230721/5270
sdx20_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX2-230721/5271
sdx24_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX2-230721/5272
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX2-230721/5273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX2-230721/5274
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX2-230721/5275
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX2-230721/5276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
sdx50m_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5277
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5278
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDX5-230721/5279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5280
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5281
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1898		
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5283
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5284
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5285
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5287
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5288
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SDX5-230721/5289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5290
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5292
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5293
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1965		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5295
sdx55m_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5296
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5298
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5299
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5300
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash	https://www.qualcomm.com/compan	O-QUA-SDX5-230721/5301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5302
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5303
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5304
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SDX5-230721/5305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5306
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5307
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SDX5-230721/5308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5309
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5311
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5312
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5314
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5315
sdx55_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5317
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5318
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5320
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5321
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5322
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SDX5-230721/5323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1899	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5324
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5325
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5326
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5328
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5329
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SDX5-230721/5330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5331
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5333
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5334
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDX5-230721/5336
sdxr1_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5337
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5339
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5340
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1931		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5342
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5343
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5345
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5346
sdxr2_5g_firmware					
Out-of-	13-Jul-21	7.2	Incorrect handling of	https://ww	O-QUA-SDXR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/5347
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5348
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5349
Improper	13-Jul-21	7.2	Improper length check of	https://ww	O-QUA-SDXR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/5350
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5351
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5352
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SDXR-230721/5353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5354
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5355
Reachable	13-Jul-21	5	Improper handling of	https://ww	O-QUA-SDXR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/5356
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5357
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5359
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SDXR-230721/5360
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SDXR-230721/5361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	bulletin	
sd_455_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_4-230721/5362
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_4-230721/5363
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD_4-230721/5364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_4-230721/5365
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_4-230721/5366
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD_4-230721/5367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_4-230721/5368
sd_636_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5370
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5371
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5373
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5374
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1938**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5376
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5377
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5379
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5381
sd_675_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5382
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5384
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5385
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5386
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SD_6-230721/5387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5388
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5389
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5390
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD_6-230721/5391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	security/bulletins/july-2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5392
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5393
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of	https://www.qualcomm.	O-QUA-SD_6-230721/5394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5395
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5397
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5398
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD_6-230721/5399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	etins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_6-230721/5400
sd_8cx_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5401
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SD_8-230721/5402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5403
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5404
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5406
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5407
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5409
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5410
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5412
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5413
sd_8c_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD_8-230721/5414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	etins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5415
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5416
Improper Restriction of Operations within the	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD_8-230721/5417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	etins/july-2021-bulletin	
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5418
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5419
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5421
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5422
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5424
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SD_8-230721/5426
sm4125_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM41-230721/5427
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM41-230721/5428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM41-230721/5429
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM41-230721/5430
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM41-230721/5431
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while	https://www.qualcomm.	O-QUA-SM41-230721/5432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM41-230721/5433
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM41-230721/5434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM41-230721/5435
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM41-230721/5436
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	O-QUA-SM41-230721/5437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM41-230721/5438
sm6250p_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5439
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function	https://www.qualcomm.	O-QUA-SM62-230721/5440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	com/company/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5441
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5442
Buffer Copy without Checking	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while	https://www.qualcomm.com/compan	O-QUA-SM62-230721/5443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5444
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5445
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in	https://www.qualcomm.com/compan	O-QUA-SM62-230721/5446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	y/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5447
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1970		
sm6250_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5449
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5450
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5452
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5453
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5454
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SM62-230721/5455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5456
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5457
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5458
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SM62-230721/5459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	2021-bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5460
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5461
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SM62-230721/5462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5463
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5465
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5466
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SM62-230721/5467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM62-230721/5468
sm7250p_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5469
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5471
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5472
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5474
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5475
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5477
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5478
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM72-230721/5479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5480
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM72-230721/5482
sm7315_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5483
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5484
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SM73-230721/5485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5486
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5487
Reachable	13-Jul-21	5	Improper handling of	https://ww	O-QUA-SM73-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/5488
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5489
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5491
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5492
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SM73-230721/5493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	bulletin	
sm7325p_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5494
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5495
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-SM73-230721/5496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5497
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5498
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5500
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5501
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5503
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5504
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when	https://www.qualcomm.com/compan	O-QUA-SM73-230721/5505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5506
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-SM73-230721/5507
Improper	13-Jul-21	5	Possible out of bound read	https://ww	O-QUA-SM73-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	230721/5508
wcd9306_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5509
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5510
Buffer Copy	13-Jul-21	7.2	Possible buffer overflow due	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCD9-230721/5511
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5512
wcd9326_firmware					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5513
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-WCD9-230721/5514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5515
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5516
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5517
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCD9-230721/5518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5519
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5520
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-WCD9-230721/5521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5522
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5524
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5525
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCD9-230721/5526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	bulletin	
wcd9330_firmware					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5527
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5528
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5529
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in	https://www.qualcomm.com/company/product-	O-QUA-WCD9-230721/5530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	security/bulletins/july-2021-bulletin	
wcd9335_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5531
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5533
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5534
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5535
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot	https://www.qualcomm.com/company/product-	O-QUA-WCD9-230721/5536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5537
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5538
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while	https://www.qualcomm.com/company/product-	O-QUA-WCD9-230721/5539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5540
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5542
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5543
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCD9-230721/5544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	bulletin	
wcd9340_firmware					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5545
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5546
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5547
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-230721/5548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5549
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5550
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5552
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5553
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5555
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5556
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	O-QUA-WCD9-230721/5557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5558
wcd9341_firmware					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5559
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1897**		
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5561
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5562
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5563
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5565
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5566
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5568
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5569
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5571
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5572
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing	https://www.qualcomm.com/compan	O-QUA-WCD9-230721/5573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5574
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5575
wcd9360_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-230721/5576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	etins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5577
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5578
Improper Restriction of Operations within the	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-230721/5579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5580
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1953**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5582
wcd9370_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5583
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCD9-230721/5584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5585
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5586
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCD9-230721/5587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5588
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5589
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5590
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1907		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5592
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5593
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1940		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5595
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5596
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5598
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5599
Improper	13-Jul-21	5	Possible buffer over read	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCD9-230721/5600
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5601
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5602
wcd9371_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	O-QUA-WCD9-230721/5603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5604
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5605
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	O-QUA-WCD9-230721/5606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5607
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5608
Out-of-	13-Jul-21	5	Possible out of bound read	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCD9-230721/5609
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5610
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5612
wcd9375_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5613
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCD9-230721/5614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5615
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5616
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCD9-230721/5617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5618
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5619
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5620
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1907		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5622
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5623
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1940		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5625
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5626
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5628
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5629
Improper	13-Jul-21	5	Possible buffer over read	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCD9-230721/5630
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5631
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5632
wcd9380_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import	https://www.qualcomm.com/compan	O-QUA-WCD9-230721/5633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	y/product-security/bulletins/july-2021-bulletin	
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5634
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5635
Improper Restriction of	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could	https://www.qualcomm.com/compan	O-QUA-WCD9-230721/5636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5637
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5638
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5640
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5641
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5642
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5644
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5645
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCD9-230721/5646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5647
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5649
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5650
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1965		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5652
wcd9385_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5653
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5655
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5656
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5657
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot	https://www.qualcomm.com/company/product-	O-QUA-WCD9-230721/5658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5659
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5660
Out-of-	13-Jul-21	5	Possible out of bound read	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCD9-230721/5661
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5662
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5664
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5665
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-WCD9-230721/5666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCD9-230721/5667
wcn3610_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5668
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN3-230721/5669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5670
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5671
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCN3-230721/5672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5673
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5674
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5675
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1940**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5677
wcn3615_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5678
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN3-230721/5679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5680
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5681
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCN3-230721/5682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5683
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5684
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5685
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1907		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5687
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5688
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5690
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5691
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-230721/5692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	etins/july-2021-bulletin	
wcn3620_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5693
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5694
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-230721/5695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5696
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5697
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1898		
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5699
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5700
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5701
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
wcn3660b_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5703
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5704
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-230721/5705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5706
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5707
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1898		
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5709
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5710
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5711
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
wcn3660_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5713
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5714
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-230721/5715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	etins/july-2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5716
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5717
wcn3680b_firmware					
Out-of-bounds	13-Jul-21	7.2	Incorrect handling of pointers in trusted	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	com/company/product-security/bulletins/july-2021-bulletin	230721/5718
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5719
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5720
Improper Restriction	13-Jul-21	7.2	Improper length check of public exponent in RSA	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	com/company/product-security/bulletins/july-2021-bulletin	230721/5721
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5722
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5723
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5725
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5726
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5727
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCN3-230721/5728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5729
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5730
Improper Input	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	com/company/product-security/bulletins/july-2021-bulletin	230721/5731
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5732
wcn3680_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5733
Double Free	13-Jul-21	7.2	Memory corruption in key	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN3-230721/5734
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5735
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5736
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	com/company/product-security/bulletins/july-2021-bulletin	230721/5737
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5738
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5739
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5740
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in	https://www.qualcomm.com/company/product-	O-QUA-WCN3-230721/5741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	security/bulletins/july-2021-bulletin	
wcn3910_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5742
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5744
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5745
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5746
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot	https://www.qualcomm.com/company/product-	O-QUA-WCN3-230721/5747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5748
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5749
Out-of-	13-Jul-21	5	Possible out of bound read	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN3-230721/5750
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5751
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5753
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5754
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-WCN3-230721/5755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5756
wcn3950_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5757
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN3-230721/5758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5759
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5760
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCN3-230721/5761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5762
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5763
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5764
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1907		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5766
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5767
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1940		
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5769
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5770
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5772
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5773
Improper	13-Jul-21	5	Possible buffer over read	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN3-230721/5774
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5775
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5776
wcn3980_firmware					
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when	https://www.qualcomm.com/compan	O-QUA-WCN3-230721/5777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	y/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5778
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5779
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5780
Buffer Copy without Checking Size of Input ('Classic	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-230721/5781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5782
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5783
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCN3-230721/5784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5785
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5786
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCN3-230721/5787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5788
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1955		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5790
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5791
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5792
wcn3988_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5793
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5794
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5796
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5797
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5798
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN3-230721/5799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2021-1899**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5800
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5801
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5802
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCN3-230721/5803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	bulletin	
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5804
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5805
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-230721/5806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	etins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5807
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1954		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5809
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5810
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1965**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5812
wcn3990_firmware					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5813
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5814
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN3-230721/5815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5816
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5817
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN3-230721/5818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5819
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5821
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5822
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5824
wcn3991_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5825
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCN3-230721/5826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5827
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5828
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5830
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5831
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5832
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5833
Buffer Copy without	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	com/company/product-security/bulletins/july-2021-bulletin	230721/5834
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5835
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5836
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-WCN3-230721/5837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5838
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5839
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while	https://www.qualcomm.com/company/product-	O-QUA-WCN3-230721/5840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5841
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5843
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5844
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1970		
wcn3998_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5846
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5847
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5849
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5850
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5851
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN3-230721/5852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5853
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5854
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5855
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**		
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5857
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5858
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5860
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5861
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	O-QUA-WCN3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	com/company/product-security/bulletins/july-2021-bulletin	230721/5862
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5863
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5865
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5866
wcn3999_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1886		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5868
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5869
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5871
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5872
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5874
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5875
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN3-230721/5877
wcn6740_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5878
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN6-230721/5879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	etins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5880
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5881
Buffer Copy without Checking Size of Input ('Classic Buffer	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN6-230721/5882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5883
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5884
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5886
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5887
Out-of-	13-Jul-21	5	Possible buffer over read	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN6-230721/5888
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5889
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5891
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5892
wcn6745_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5894
wcn6750_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5895
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the	https://www.qualcomm.com/compan	O-QUA-WCN6-230721/5896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	y/product-security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5897
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5898
Buffer Copy without Checking Size of Input	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-WCN6-230721/5899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5900
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5901
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN6-230721/5902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5903
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1953		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5905
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5906
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5908
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5909
wcn6850_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5911
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5912
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**		
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5914
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5915
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5916
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WCN6-230721/5917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5918
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5919
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR	https://www.qualcomm.	O-QUA-WCN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	com/company/product-security/bulletins/july-2021-bulletin	230721/5920
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5921
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5923
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5924
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**		
wcn6851_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5926
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5927
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5929
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5930
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5932
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5933
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5935
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5936
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when	https://www.qualcomm.com/compan	O-QUA-WCN6-230721/5937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	y/product-security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5938
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5939
Improper	13-Jul-21	5	Possible out of bound read	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN6-230721/5940
wcn6855_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5941
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5942
Buffer Copy	13-Jul-21	7.2	Possible buffer overflow due	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN6-230721/5943
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5944
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5945
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WCN6-230721/5946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5947
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5949
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5950
wcn6856_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1886**		
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5952
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5953
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1890		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5955
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5956
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5957
Out-of-	13-Jul-21	5	Possible buffer out of bound	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	WCN6-230721/5958
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5959
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**		
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5961
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5962
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in	https://www.qualcomm.com/company/product-	O-QUA-WCN6-230721/5963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5964
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WCN6-230721/5965
whs9410_firmware					
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WHS9-230721/5966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	2021-bulletin	
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WHS9-230721/5967
wsa8810_firmware					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-230721/5968
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of	https://www.qualcomm.	O-QUA-WSA8-230721/5969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	com/company/product-security/bulletins/july-2021-bulletin	
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-230721/5970
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-230721/5971
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-230721/5972
Buffer Copy without Checking Size of Input	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-WSA8-230721/5973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	security/bulletins/july-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-230721/5974
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-230721/5975
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WSA8-230721/5976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-230721/5977
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-230721/5978
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WSA8-230721/5979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	2021-bulletin	
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5980
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1955**		
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5982
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5983
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wsa8815_firmware					
N/A	13-Jul-21	3.3	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity **CVE ID : CVE-2021-1896**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5985
Out-of-bounds Read	13-Jul-21	2.1	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1897**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5986
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1898**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5987
Out-of-bounds Read	13-Jul-21	2.1	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1899**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5988
Out-of-	13-Jul-21	2.1	Possible buffer over-read	https://ww	O-QUA-WSA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1901**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	240721/5989
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5990
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5991
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**		
Use After Free	13-Jul-21	7.2	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1940**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5993
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5994
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**		
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5996
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5997
Reachable	13-Jul-21	5	Denial of service in SAP case	https://ww	O-QUA-WSA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	240721/5998
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/5999
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1965		
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6001
wsa8830_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6002
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1888		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6004
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6005
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2021-1907**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6006
Buffer Copy without Checking Size of Input	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot	https://www.qualcomm.com/company/product-	O-QUA-WSA8-240721/6007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6008
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6009
Out-of-	13-Jul-21	5	Possible out of bound read	https://ww	O-QUA-WSA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	w.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	240721/6010
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6011
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**		
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6013
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1964**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6014
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-WSA8-240721/6015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	security/bulletins/july-2021-bulletin	
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6016
wsa8835_firmware					
Out-of-bounds Write	13-Jul-21	7.2	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1886**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6017
Double Free	13-Jul-21	7.2	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-WSA8-240721/6018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1888**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1889**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6019
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-Jul-21	7.2	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1890**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6020
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	5	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-	O-QUA-WSA8-240721/6021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile **CVE ID : CVE-2021-1907**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Jul-21	7.2	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1931**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6022
Reachable Assertion	13-Jul-21	5	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1938**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6023
Out-of-bounds Read	13-Jul-21	5	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1943**		
Out-of-bounds Read	13-Jul-21	5	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1945**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6025
Reachable Assertion	13-Jul-21	5	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1953**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6026
Out-of-bounds Read	13-Jul-21	5	Possible buffer over read due to improper validation	https://www.qualcomm.	O-QUA-WSA8-240721/6027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1954**	com/company/product-security/bulletins/july-2021-bulletin	
Reachable Assertion	13-Jul-21	5	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1955**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6028
Improper Input Validation	13-Jul-21	5	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1964**		
Improper Input Validation	13-Jul-21	10	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1965**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6030
Improper Input Validation	13-Jul-21	5	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2021-1970**	https://www.qualcomm.com/company/product-security/bulletins/july-2021-bulletin	O-QUA-WSA8-240721/6031
Redhat					
enterprise_linux					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-21	8	A flaw was found in the ptp4l program of the linuxptp package. A missing length check when forwarding a PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and	https://bugzilla.redhat.com/show_bug.cgi?id=1966240	O-RED-ENTE-240721/6032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before 2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1. **CVE ID : CVE-2021-3570**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-21	5.5	A flaw was found in the ptp4l program of the linuxptp package. When ptp4l is operating on a little-endian architecture as a PTP transparent clock, a remote attacker could send a crafted one-step sync message to cause an information leak or crash. The highest threat from this vulnerability is to data confidentiality and system availability. This flaw affects linuxptp versions before 3.1.1 and before 2.0.1. **CVE ID : CVE-2021-3571**	https://bugzilla.redhat.com/show_bug.cgi?id=1966241	O-RED-ENTE-240721/6033
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Jul-21	2.1	There's a flaw in OpenEXR's ImfDeepScanLineInputFile functionality in versions prior to 3.0.5. An attacker who is able to submit a crafted file to an application linked with OpenEXR could cause an out-of-bounds read. The greatest risk from this flaw is to application availability. **CVE ID : CVE-2021-3598**	https://bugzilla.redhat.com/show_bug.cgi?id=1970987	O-RED-ENTE-240721/6034
Improper Restriction of	09-Jul-21	7.2	An out-of-bounds memory write flaw was found in the Linux kernel's joystick	https://lore.kernel.org/linux-	O-RED-ENTE-240721/6035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			devices subsystem in versions before 5.9-rc1, in the way the user calls ioctl JSIOCSBTNMAP. This flaw allows a local user to crash the system or possibly escalate their privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2021-3612**	input/20210620120030.1513655-1-avlarkin82@gmail.com/	
enterprise_linux_aus					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-21	8	A flaw was found in the ptp4l program of the linuxptp package. A missing length check when forwarding a PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before 2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1. **CVE ID : CVE-2021-3570**	https://bugzilla.redhat.com/show_bug.cgi?id=1966240	O-RED-ENTE-240721/6036
enterprise_linux_eus					
Improper Restriction of Operations	09-Jul-21	8	A flaw was found in the ptp4l program of the linuxptp package. A missing length check when	https://bugzilla.redhat.com/show_bug.cgi?id=1966	O-RED-ENTE-240721/6037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			forwarding a PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before 2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1. **CVE ID : CVE-2021-3570**	240	
enterprise_linux_tus					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jul-21	8	A flaw was found in the ptp4l program of the linuxptp package. A missing length check when forwarding a PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before 2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1. **CVE ID : CVE-2021-3570**	https://bugzilla.redhat.com/show_bug.cgi?id=1966240	O-RED-ENTE-240721/6038
Rockwellautomation					
micrologix_1100_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jul-21	5	Rockwell Automation MicroLogix 1100, all versions, allows a remote, unauthenticated attacker sending specially crafted commands to cause the PLC to fault when the controller is switched to RUN mode, which results in a denial-of-service condition. If successfully exploited, this vulnerability will cause the controller to fault whenever the controller is switched to RUN mode. **CVE ID : CVE-2021-33012**	N/A	O-ROC-MICR-240721/6039
selinux_project					
selinux					
Use After Free	01-Jul-21	2.1	The CIL compiler in SELinux 3.2 has a use-after-free in __cil_verify_classperms (called from __cil_verify_classpermission and __cil_pre_verify_helper). **CVE ID : CVE-2021-36084**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=31065, https://github.com/SELinuxProject/selinux/commit/f34d3d30c8325e4847a6b696fe7a3936a8a361f3	O-SEL-SELI-240721/6040
Use After Free	01-Jul-21	2.1	The CIL compiler in SELinux 3.2 has a use-after-free in __cil_verify_classperms (called from __verify_map_perm_classperms and hashtab_map). **CVE ID : CVE-2021-36085**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=31124, https://githu	O-SEL-SELI-240721/6041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				b.com/SELinuxProject/selinux/commit/2d35fcc7e9e976a2346b1de20e54f8663e8a6cba	
Use After Free	01-Jul-21	3.6	The CIL compiler in SELinux 3.2 has a use-after-free in cil_reset_classpermission (called from cil_reset_classperms_set and cil_reset_classperms_list). **CVE ID : CVE-2021-36086**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=32177, https://github.com/SELinuxProject/selinux/commit/c49a8ea09501ad66e799ea41b8154b6770fec2c8	O-SEL-SELI-240721/6042
Out-of-bounds Read	01-Jul-21	2.1	The CIL compiler in SELinux 3.2 has a heap-based buffer over-read in ebitmap_match_any (called indirectly from cil_check_neverallow). NOTE: bad0a746e9f4cf260dedba5828d9645d50176aac is cited in the OSV "fixed" field but does not have a code change. **CVE ID : CVE-2021-36087**	https://github.com/SELinuxProject/selinux/commit/bad0a746e9f4cf260dedba5828d9645d50176aac, https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=32675	O-SEL-SELI-240721/6043
tieline					
ip_audtio_gateway_firmware					
Incorrect Authorizatio	01-Jul-21	7.5	Tieline IP Audio Gateway 2.6.4.8 and below is affected	N/A	O-TIE-IP_A-240721/6044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			by Incorrect Access Control. A vulnerability in the Tieline Web Administrative Interface could allow an unauthenticated user to access a sensitive part of the system with a high privileged account. **CVE ID : CVE-2021-35336**		
Zyxel					
usg1000_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG1-240721/6045
usg100_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG1-240721/6046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
usg1100_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG1-240721/6047
usg110_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG1-240721/6048
usg1900_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG1-240721/6049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**		
usg20-vpn_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG2-240721/6050
usg2000_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG2-240721/6051
usg200_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex,	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_agains	O-ZYX-USG2-240721/6052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	t_security_appliances.shtml	
usg20w-vpn_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG2-240721/6053
usg20w_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG2-240721/6054
usg20_firmware					
Improper Authenticati	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-	https://www.zyxel.com/	O-ZYX-USG2-240721/6055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	
usg210_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG2-240721/6056
usg2200-vpn_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG2-240721/6057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
usg300_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG3-240721/6058
usg310_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG3-240721/6059
usg40w_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG4-240721/6060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**		
usg40_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG4-240721/6061
usg50_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG5-240721/6062
usg60w_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex,	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_agains	O-ZYX-USG6-240721/6063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	t_security_appliances.shtml	
usg60_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG6-240721/6064
usg_flex_100w_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG_-240721/6065
usg_flex_100_firmware					
Improper Authenticati	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-	https://www.zyxel.com/	O-ZYX-USG_-240721/6066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	
usg_flex_200_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG_-240721/6067
usg_flex_500_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG_-240721/6068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
usg_flex_700_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-USG_-240721/6069
zywall_1100_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-ZYWA-240721/6070
zywall_110_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-ZYWA-240721/6071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**		
zywall_310_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-ZYWA-240721/6072
zywall_atp100w_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-ZYWA-240721/6073
zywall_atp100_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex,	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_agains	O-ZYX-ZYWA-240721/6074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	t_security_appliances.shtml	
zywall_atp200_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-ZYWA-240721/6075
zywall_atp500_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-ZYWA-240721/6076
zywall_atp700_firmware					
Improper Authenticati	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-	https://www.zyxel.com/	O-ZYX-ZYWA-240721/6077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	
zywall_atp800_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-ZYWA-240721/6078
zywall_vpn100_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-ZYWA-240721/6079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
zywall_vpn300_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-ZYWA-240721/6080
zywall_vpn50_firmware					
Improper Authentication	02-Jul-21	7.5	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device. **CVE ID : CVE-2021-35029**	https://www.zyxel.com/support/Zyxel_security_advisory_for_attacks_against_security_appliances.shtml	O-ZYX-ZYWA-240721/6081